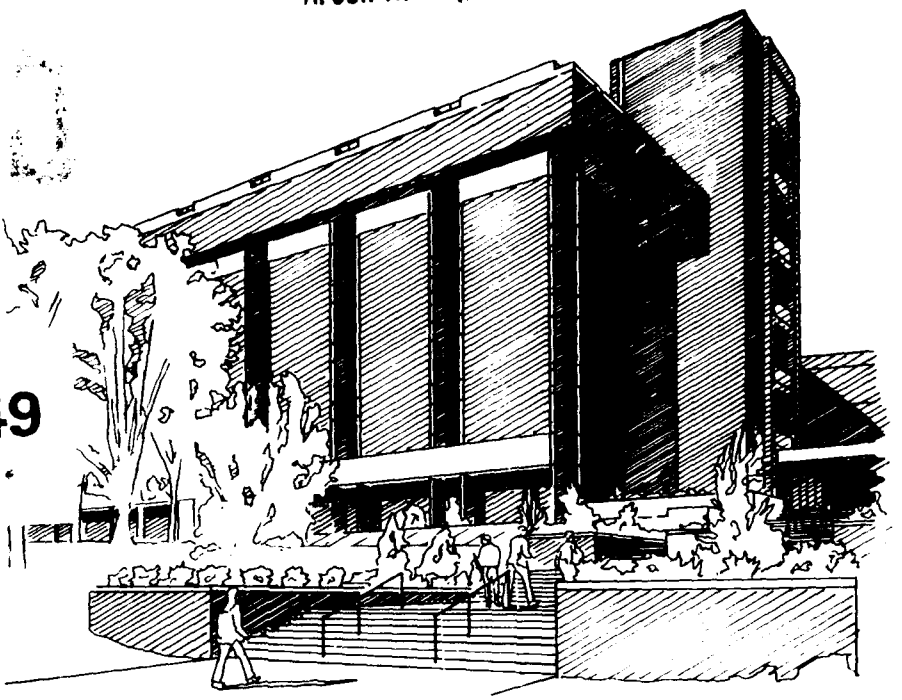


UNIVERSITY OF CINCINNATI
COLLEGE OF ENGINEERING

APPROXIMATE EVALUATION OF RELIABILITY AND AVAILABILITY VIA PERTURBATION ANALYSIS

Final Technical Report on
Grant AFOSR-89-0486

December, 1990

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION Unclassified	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY N/A	3. DISTRIBUTION/AVAILABILITY OF REPORT Approved for Public Release; Distribution Unlimited
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE N/A	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) N/S	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION University of Cincinnati Dept. of Aerospace Eng. 6b. OFFICE SYMBOL (If applicable)	7a. NAME OF MONITORING ORGANIZATION AFOSR/NM
6c. ADDRESS (City, State, and ZIP Code) Mail Location 343 University of Cincinnati Cincinnati, Ohio 45221-0343	7b. ADDRESS (City, State, and ZIP Code) Building 410 Bolling AFB, DC 20332-6448
8a. NAME OF FUNDING/SPONSORING ORGANIZATION AFOSR 8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER AFOSR-89-0486
8c. ADDRESS (City, State, and ZIP Code) Building 410 Bolling AFB, DC 20332-6448	10. SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO. 6.1102F; PROJECT NO. 2304; TASK NO. A5; WORK UNIT ACCESSION NO.

11. TITLE (Include Security Classification)
Approximate Evaluation of Reliability and Related Quantities Via Perturbation Techniques

12. PERSONAL AUTHOR(S)
B.K. Walker & R. Srichander

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (Year, Month, Day)	15. PAGE COUNT
Final	FROM 01SEP89 TO 30SEP90	1990 December	105

16. SUPPLEMENTARY NOTATION

17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	Reliability evaluation; fault tolerant systems; stochastic stability; semi-Markov models

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

The evaluation of the reliability, stability, and performance of fault tolerant control systems (FTCS) is considered. New sufficient conditions for stochastic stability of FTCS with standard Markovian component failure behavior and Markovian failure detection decision behavior are derived. By specializing these results to the class of linear time-invariant (LTI) FTCS with linear state feedback control laws that are reconfigured by switching the feedback gain matrix according to the identified failure configuration, the stability results are strengthened to necessary and sufficient conditions for stochastic stability of a special type (exponential in mean square) that implies a very strong sense of stability (a.s. in probability). An approximate feedback control design technique for LTI FTCS is then proposed and demonstrated on a simple numerical case.

In addition, previous results on semi-Markov analysis of FTCS reliability are used to derive a numerical method for establishing approximately optimal failure detection test thresholds for sequential failure detection tests. This method, though approximate, is shown to yield thresholds that provide a considerable increase in system reliability relative to those provided by a method based on a rigorously derived reliability approximation for one numerical example.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS	21. ABSTRACT SECURITY CLASSIFICATION Unclassified
22a. NAME OF RESPONSIBLE INDIVIDUAL Dr. Jon A. Sjogren	22b. TELEPHONE (Include Area Code) (202)767-4940 22c. OFFICE SYMBOL AFOSR/NM

DD FORM 1473, 84 MAR 83 APR edition may be used until exhausted. All other editions are obsolete.

SECURITY CLASSIFICATION OF THIS PAGE
UNCLASSIFIED

APPROXIMATE EVALUATION OF RELIABILITY AND RELATED QUANTITIES VIA PERTURBATION TECHNIQUES

Final Technical Report on

Grant AFOSR-89-0486

Prof. Bruce K. Walker

Dr. Ramaswamy Srichander

Dept. of Aerospace Engineering & Engineering Mechanics
University of Cincinnati
Cincinnati, OH 45221-0343

December, 1990

Covering the Period: September 1, 1989 - September 30, 1990

Prepared for:
Dr. Jon A. Sjogren
AFOSR/NM
Building 410
Bolling AFB, DC 20332-6448

TABLE OF CONTENTS

ABSTRACT

The evaluation of the reliability, stability, and performance of fault tolerant control systems (FTCS) is considered. New sufficient conditions for stochastic stability of FTCS with standard Markovian component failure behavior and Markovian failure detection decision behavior are derived. By specializing these results to the class of linear time-invariant (LTI) FTCS with linear state feedback control laws that are reconfigured by switching the feedback gain matrix according to the identified failure configuration, the stability results are strengthened to necessary and sufficient conditions for stochastic stability of a special type (exponential in mean square) that implies a very strong sense of stability (a.s. in probability). An approximate feedback control design technique for LTI FTCS is then proposed and demonstrated on a simple numerical case.

In addition, previous results on semi-Markov analysis of FTCS reliability are used to derive a numerical method for establishing approximately optimal failure detection test thresholds for sequential failure detection tests. This method, though approximate, is shown to yield thresholds that provide a considerable increase in system reliability relative to those provided by a method based on a rigorously derived reliability approximation for one numerical case.

1. INTRODUCTION

1.1 Motivation and Discussion of Problem

The evaluation of the reliability, performance, and stability properties of fault tolerant control systems (FTCS) is problematic due to several characteristics of these systems. Fundamentally, the behavior of FTCSs is probabilistic in nature. The random nature of the behavior stems from the random occurrence of failures, the random noise disturbing the system and corrupting its outputs, and the interaction of the failure detection and isolation (FDI) logic with the noise-corrupted outputs. This means that any evaluation technique must account for all of the random behavior to which FTCS are subject.

Most of the evaluation methods that have found success for FTCS are based upon Markov modeling. The failure behavior of the components comprising most FTCS is usually well-modeled by a Markov jump process, and if the correlations between component failure events (if any) are known, then the system failure configuration can be modeled by a finite-state Markov jump process. The random noise corrupting the measurements is often modeled as white (i.e. as if uncorrelated in time). If the FDI tests used by the system are instantaneous, such as the standard threshold tests or instantaneous parity equation tests based on analytic redundancy, then the FDI decision behavior is also Markovian when conditioned on the failure configuration. This situation lends itself to a Markov jump process model of the FTCS behavior from which the system reliability and performance can be derived, provided the interaction between the FDI logic and the system configuration is properly accounted for [1]. The problem for the FTCS evaluator is then one of solving for the transient behavior of the resulting Markov model. The transient solution is often complicated by the large number of states possessed by typical FTCS models and by large ranges in the transition rates of the model due to the often extremely slow rate of component failures relative to the rate at which FDI decisions are made.

The Markov jump process modeling technique breaks down when the FDI tests involve memory. Any sequential FDI test (such as Wald's sequential probability ratio test, the Shiryaev test, or any likelihood ratio test based upon a history of measurements) and any test involving dynamic filtering of the measurement data (such as the detection filter, the dedicated observer approach, and the unknown input filter) no longer behaves

in a Markovian fashion even if the noise corrupting the measurements in use is white. In many of these cases, however, the FDI decision behavior can be modeled by a finite state semi-Markov process conditioned on the failure behavior. When combined with the Markovian failure characterization, the result is a semi-Markov model for the FTCS behavior that yields reliability and performance information if the transient solution to the model can be calculated [2].

Much of our previous work has dealt with the difficulty of solving for the transient behavior of semi-Markov FTCS behavior models [3-8]. These solution difficulties arise from the sources cited above (large number of model states, wide range of transition rates) and also from the convolutions necessary to evaluate the transient solution to semi-Markov models. The work described in [3-8] was directed toward approximating the transient solution by simpler forms obtained by exploiting the wide discrepancy that typically exists between the failure rates of the components and the FDI decision rates to decompose the semi-Markov model into aggregate classes. The reader is referred to [3-8] for further details and results.

In the work reported here, we shift our attention slightly to the problem of evaluating stability properties of FTCS and to determining thresholds for sequential FDI tests that are commonly used in FTCS. The stability issue, like the reliability and performance evaluation problem, is complicated by the fact that FTCS are fundamentally stochastic systems. Therefore, stability for FTCS must be defined in a stochastic sense and the theory of stochastic stability must be employed to derive results. The threshold determination issue, which we have addressed for a special type of system [9-10], is related more closely to our reliability evaluation work because the reliability is often the measure by which the FDI threshold selection is judged.

1.2 Previous and Related Work

As discussed above, our own previous work and that of others (reported in [3-8] and the references thereof) has focused primarily on the reliability evaluation problem for FTCS. We have examined the threshold determination problem before [9-10], but only for the case of instantaneous FDI tests. To our knowledge, the threshold determination procedure for sequential FDI tests discussed later in this report is unprecedented in the literature on FTCS.

The stability question for FTCS has been studied in recent years by several other researchers. Our work is closely related to that of Mariton, reported in [11], who examined the stochastic stability of FTCS under the assumption that the FDI decisions could be delayed by a random time but were always correct. Our results also are related slightly to those reported by Ji and Chizeck in [12] for the special case of FTCS called the jump linear quadratic regulator (JLQR) problem with the assumption that the FDI decisions are always correct and delayed by no more than one time step. In fact, our results are generalizations of the results of both of these references, as we shall show.

1.3 Outline of Report

The remainder of this report is laid out as follows. The next section presents a detailed summary of our research findings. These results are presented in the form of manuscripts included as subsections of the next section, each preceded by a brief introduction to its contents. Section 3 summarizes the major findings reported in Section 2. The personnel involved in the project are listed in Section 4. Section 5 lists the publications and presentations that resulted from this work and from the previous AFOSR-supported work that appeared during the project period. Finally, the references are listed in Section 6.

2. PROGRESS SUMMARY

In this section, we present a detailed summary of the technical work accomplished under the grant. Because they concisely summarize our results and relate our work to the work of other researchers, we rely almost entirely in this section on the manuscripts of three papers written under the grant and submitted for publication. (See Section 5 on papers and presentations.) To place these manuscripts in perspective, each is preceded by a brief description of its contents and its relationship to the other work accomplished under the grant.

2.1 Determination of Approximately Optimal Sequential Test Thresholds

This work most closely follows from the work on reliability analysis that we accomplished under previous grants [3-8]. Basically, the assumption is made that a semi-Markov model has been constructed that describes the behavior of a FTCS including random failures and FDI decision delays and errors. If this model is to be used to determine the test thresholds that minimize the system unreliability at some fixed duration, then ordinarily a numerical optimization scheme like a gradient approach must be used. Such schemes require many evaluations of the model, each of which is very time-consuming. In this manuscript, we suggest a simpler method for determining the thresholds that requires the evaluation only of a few of the transition probability mass functions in the semi-Markov model instead of the entire model behavior. As we demonstrate for one numerical case, the resulting thresholds can be better in terms of the system reliability that results from their use than thresholds determined by other means.

SELECTING THRESHOLDS FOR SEQUENTIAL FAULT DETECTION TESTS

R. Srichander

Center for Artificial Intelligence and Robotics, Bangalore, India

Bruce K. Walker

Health Monitoring Technology Center, Department of Aerospace Engineering and Engineering Mechanics, University of Cincinnati, Cincinnati, Ohio, USA

Abstract. Many redundancy management (RM) algorithms use sequential tests for detecting and identifying component failures because the sequential processing of noisy data samples often results in significant decreases in the probabilities of false detection and of missed detection relative to single sample tests. However, this improvement in the error probabilities comes at the cost of a larger delay in detecting or identifying a failure. The error probabilities and delay statistics characterize the performance of the sequential tests, and these performance properties play a crucial role in determining the overall fault tolerant system performance. In this paper, a simple technique to derive approximately optimum thresholds for sequential failure detection tests is indicated where the performance of the fault tolerant control system is the optimality criterion. The threshold selection method is illustrated by a generic quadraplex redundant system example.

Keywords. Failure detection; reliability; redundancy; fault tolerant systems; Markov processes; thresholds; sequential tests.

INTRODUCTION

In recent years, redundancy of critical components has been used to enhance the reliability of control systems for many applications. Examples include aircraft flight control systems (Moerder and others, 1989; Howell and others, 1983; Looze and others, 1985), spacecraft attitude control and inertial navigation systems (Harrison and others, 1979; Kerr, 1987) and nuclear power plant operating systems (Gai, Harrison, & Deyst, 1981). For each of these applications, high reliability is of prime importance, which in turn motivates the use of active fault tolerant control systems. An active fault tolerant control system comprises a redundant set of hardware components and a fully automated redundancy management (RM) algorithm to reconfigure the system in real time when component failures occur. One of the functions of the RM algorithm is the detection and identification of failures. This is usually accomplished through the use of statistical failure detection and identification (FDI) tests combined with automatic logic to process the test outcomes.

The reliability of a fault tolerant system is determined not only by the reliabilities of its individual components but also by the FDI test statistics. For instance, the reliability of a fault tolerant system comprised of very reliable components but with a fault detection algorithm prone to false alarms can be unacceptably low. In such a case, false alarms can be so frequent that the effective redundancy level of the system is reduced. The motivation for the work reported here stems from the fact that the overall fault tolerant system performance can be enhanced by improving the performance of the FDI tests.

Markovian models have been used in recent times to assess the reliability and performance of fault tolerant systems that use FDI tests of the single sample variety (Walker & Gai, 1979). Single sample FDI tests are tests that use only data obtained at a single time instant, as opposed to tests that use data obtained over a fixed or variable window of several time samples. The determination of optimum thresholds for systems using single sample tests has been examined by Harrison and others (1979). However, single sample FDI tests often have high probabilities of error, particularly in noisy signal environments, that may lead to unacceptable system

reliabilities. To overcome this drawback, moving window and sequential tests have been suggested for FDI (Willsky, 1976). The improvement in the error probabilities for these tests comes at the cost of a larger delay in detecting and identifying a failure.

By their nature, sequential tests are not memoryless. Therefore, Markov models are not applicable for evaluating the performance of systems that use them. Instead, semi-Markov models can be used to evaluate the performance quantities of interest for a broad class of fault tolerant systems that use sequential FDI tests (Walker, 1980). However, semi-Markov models are often computationally intractable because of their large dimension, the presence of convolution sums in the calculations, and the long time periods that are typically of interest in fault tolerant systems applications. The decomposition of semi-Markov models to make practical the approximate evaluation of the reliability of fault tolerant systems over long mission times has been described by Wereley (1987), Walker, Chu & Wereley (1988), and Srichander & Walker (1989).

The present work is aimed at deriving thresholds for sequential FDI tests which can improve the overall performance and reliability of a fault tolerant system. In current practice, these thresholds are often either fixed at the 3σ level of the noise in the measurements or based on Monte Carlo simulation results. Simulation experiments are very expensive at the design phase. Time varying noise statistics are also difficult to account for with these methods. Thresholds have also been chosen based upon single test performance probabilities (i.e. the probability that each test will produce a false or missed alarm), but these methods do not take into consideration the structure of the FDI logic and hence do not capture the effect of the thresholds on the overall system performance . In the case of sequential tests, we are also often interested in minimizing the average sample number (ASN) of the tests, which determines the delay in detecting failures. The ASN is usually a function of the test threshold (Wald, 1947).

In this paper, an approximate method for determining optimal thresholds for sequential FDI tests is presented and demonstrated on a quadraplex system example that uses sequential tests for FDI. The method to generate optimal failure detection thresholds is computationally inexpensive and will be seen to yield significant improvements in overall system reliability

relative to the standard 3σ thresholds.

The rest of the paper is organized as follows: In section 2, a semi-Markov model for a generic example of a quadraplex system is briefly described. Section 3 describes a method to derive optimum thresholds for sequential FDI tests based on the first passage time and state duration statistics of a semi-Markov model. Evaluation of the selected thresholds in terms of the performance of the quadraplex system and a discussion of the results are presented in section 4.

A SEMI-MARKOV PERFORMANCE MODEL EXAMPLE

The model that is used to calculate fault tolerant system performance quantities depends upon the architecture of the RM algorithm that is employed. Therefore, these models are system-specific, and it is not possible to define a "generic" model structure. In this paper, a particular quadraplex fault tolerant system architecture is discussed and analyzed. Although a specific architecture is examined, the applications of such a generic architecture are many. The architecture could, for example, represent redundant air data sensors in a flight control system. Note, however, that the concepts that are applied later in the paper for determining FDI test thresholds are applicable to *any* semi-Markov performance evaluation model where the behavior that is characterized by the model is similar to the behavior of the example system described in this section.

Quadraplex systems are quite common in high reliability environments because under ideal circumstances they are capable of "fail-op, fail-op, fail-safe" performance. In other words, they can tolerate two failures with little or no loss of performance. This section describes a particular quadraplex sensor system architecture, and the framework for a semi-Markov performance evaluation model for it is given. Note that the form of this model is rather general provided the FDI decision logic is of a particular form. The tests used for FDI are assumed to be a sequential probability ratio test (SPRT) due to Wald (1947) and a one-sided SPRT (also known as a CUSUM procedure, see Page (1954)), referred to in this paper and by Walker (1980) as a sequential ratio detection test (SRDT).

Assumed FDI Architecture

We now proceed to describe the assumed FDI logic for the quadraplex architecture we will examine. At the four-level stage when all four sensors are operational, let us denote the measurement at time sample k of each sensor by $\{m_i(k),\ i=1,2,3,4\}$. Two pairwise differences of these measurements are used to produce a residual sequence for failure detection as follows:

$$r_1(k) = m_1(k) - m_2(k)$$

$$r_2(k) = m_3(k) - m_4(k)$$

We assume that $E\{r_1(k)\}=0$ under the conditions of no failure (hypothesis H_0) and that when a failure in one of the instruments is present (hypothesis H_1), the residual sequences have the following mean values:

$E\{r_1(k)\}=\pm a$, $E\{r_2(k)\}=0$ if instrument 1 fails

$E\{r_1(k)\}=\mp a$, $E\{r_2(k)\}=0$ if instrument 2 fails

$E\{r_2(k)\}=\pm a$, $E\{r_1(k)\}=0$ if instrument 3 fails

$E\{r_2(k)\}=\mp a$, $E\{r_1(k)\}=0$ if instrument 4 fails

where $a>0$ is a constant. Under each of the hypotheses, we assume that the variances of both residual sequences are σ^2.

At the four-level stage, we will apply four SRDTs to the residual sequences in order to detect failures and identify polarity information. The SRDTs have the form:

Declare a failure is present (and specify polarity) if $S_i(k)>T_i^D$, $(i=1,2,3,4)$ otherwise continue to the next sample.

The test statistic $S_i(k)$ is given by:

$$S_i(k) = \max\{0,\ S_i(k-1)\pm r_l(k)\mp a/2\}$$

with $S_i(0)=0$ $(i=1,2,3,4)$ where $l=1$ for $i=1,2$ and $l=2$ for $i=3,4$ and the top sign is used for one test and the bottom sign is used for the other. T_i^D is the detection threshold, which is to be determined by the designer. We refer the reader to Walker (1980) for more details on the form of the test.

The logic for using the outcomes of these two tests is assumed to be as

follows. No failure is assumed to be present until at least one of the SRDTs terminates with a threshold crossing. If two or more SRDTs arrive simultaneously at a failure decision, the tests are reinitiated. Otherwise, depending on which one of the SRDTs arrived at a failure decision, one of two isolation options is triggered that uses two SPRTs for isolating the failed component. For the SPRTs, two residual sequences are formed as:

$$q_1(k) = m_1(k) - m_3(k)$$

$$q_2(k) = m_2(k) - m_4(k)$$

Each SPRT has the form:

Declare a failure if $R_i(k) > T_i^I$, $(i=1,2)$ otherwise proceed to the next sample.

Here, T_i^I is the isolation threshold, which is determined by the designer, and:

$$R_i(k) = R_i(k-1) \pm q_1(k) \mp \alpha/2$$

with $R_i(k_D)=0$ $(i=1,2)$ where k_D is the time sample at which detection occurs, and 1 and the signs on the quantities depend upon which SRDT was triggered (see Walker (1980)). If both SPRTs arrive at "no failure" decisions (H_0), the SRDTs for failure detection are reinitiated (i.e. the detection alarm is rejected as false). If only one of the SPRTs arrives at a failure decision (H_1), the corresponding instrument is isolated as failed.

When one of the instruments is isolated by the FDI logic as being failed, the remaining three instruments are redesignated 1,2, and 3. Two residual sequences $\{r_1(k)\}$ and $\{r_2(k)\}$ are again generated using pairwise differences of the observations from the instruments, in this case using instruments 1 and 2 as one pair and instruments 2 and 3 as the other. Three-level failure detection logic using SRDTs and failure isolation logic using SPRTs are used again.

When only two instruments remain operational, we assume that built in test equipment (BITE) is used on the isolated instruments in order to retrieve instruments that were isolated due to false decisions. The BITE tests are assumed to have known proabilities of false alarm and missed alarm.

Semi-Markov Model

For a system like the one described above, a semi-Markov model can be constructed to characterize the evolution of its configuration as failures and FDI events occur (Walker, 1980; Wereley, 1987). These models consist of a finite set of states that represent the various system configurations and a complete statistical description of the transition behavior among these states. For more details on developing semi-Markov reliability models, see Walker (1980) or Wereley (1987).

One of the states in a semi-Markov evaluation model is always a system loss state. A system loss results if there are unisolated failed instruments in operation whose outputs, when used to generate the control, cause a mission failure.

The state transition diagram for a semi-Markov model of the quadraplex sensor system described above is shown in Figs. 1 and 2. The semi-Markov modeling technique gives rise to a 24-state model for our quadraplex example, though in practice some of the states can be aggregated. The definitions of some of the states in the 24-state semi-Markov evaluation model include:

State 1. *Four instruments working, no failures present, no detection alarms by SRDTs present.* (Designated 4/0/0.)

State 2. *Four instruments working, no failures present, SRDT alarm has occurred, SPRTs in operation.* (Designated 4/0/D.)

State 3. *Three instruments working, no failures present, one false isolation, no detection alarms by SRDT present.* (Designated 3/FI/0.)

State 4. *Three instruments working, no failures present, one false isolation, one SRDT alarm present, SPRTs in operation.* (Designated 3/FI/0/D.)

State 5. *Two instruments working, two false isolations, BITE operating.* (Designated 2/2FI.)

For all but three of the remaining states, the state designators are given below:

6.	4/F/O.	7.	4/F/D.
8.	4/F/P.	9.	4/F/WP.
10.	3/I/O.	11.	3/F/FI/O.
12.	3/F/FI/D.	13.	3/F/FI/P.
14.	3/F/FI/WP.	15.	3/I/O/D.
16.	2/I/FI.	17.	3/F/I/O.
18.	3/F/I/P.	19.	3/F/I/WP.
20.	3/F/I/D.	21.	2/2I.

The remaining three states all result in a system loss:

State 22. *System loss due to two failures present among four working instruments.*

State 23. *System loss due to two failed instruments present among three working instruments.*

State 24. *System loss due to one failed instrument present among two working instruments.*

Fig. 1 depicts the "fast" transitions in the model, i.e. those that are not failure rate dependent. Fig. 2 shows the failure or ε-dependent transitions, where ε is the failure rate per time step of the instruments and is assumed to be much smaller than the FDI transition rates. The three system loss states are indicated in the figures.

In developing the semi-Markov model for this system, the statistics of central importance are the probability mass functions (pmf) of the decisive sample number (DSN) for the various sequential tests. (The DSN is the number of samples following test initiation until the test terminates with a decision). In general, these pmf's are not known exactly and can only be approximated numerically. One of the earliest numerical ways to approximate them for the SPRT is described by Bhate (1959). This is based on the derivation of upper and lower bounds on the pmf value at each value of the DSN of the test. More recently, a method that lends itself to recursive

numerical solutions for these mass functions using standard numerical quadrature routines was proposed by Walker (1980). For this paper, all of the DSN pmf's were evaluated using this method.

OPTIMUM THRESHOLD APPROXIMATION

The primary objective of any fault tolerant system is to maximize the probability of accomplishing the mission. A suitable performance criterion that reflects this objective is the minimization of the probability of occupying the system loss state after a given number of time samples. Considerations of this nature in developing FDI test thresholds have been examined in the case of single-sample FDI tests by formulating a Markov model for generating this probability, as first discussed by Walker and Gai (1979).

An interesting aspect of using the probability of system loss as the performance criterion is that the thresholds tend to be chosen such that the FDI decisions are delayed as long as possible in order to keep the likelihood of decision errors low. This is clearly reflected in the FDI thresholds derived for the example considered by Walker and Gai (1979), which are such that all the FDI decisions are delayed until the last segment of the mission. Thus, the use of system loss probability as a cost function takes into account the "coverage" probability, but reflects nothing about the performance degradation suffered during the delays until decisions are reached. Also, the presence of BITE to retrieve instruments falsely isolated by the FDI logic after the second detected failure has a significant impact on the coverage probabilities. Since BITE usually has relatively high probabilities of decision errors, a cost function (such as the system loss probability) that accounts for the actions of BITE in arriving at the thresholds for the sequential tests can result in degraded performance for the system despite minimizing the system loss probability. This is because the presence of BITE can result in very low threshold values for the sequential tests, which in turn implies that unfailed instruments are frequently isolated and then brought back into operation via BITE. Such frequent switching among the system configurations may be undesirable from a control point of view because it can lead to instability (Srichander, 1990).

Another aspect of the threshold determination problem that must be considered is the tractability of the optimization procedure. When Walker and Gai (1979) considered single-sample FDI tests, the numerical calculation of the time evolution of a Markovian model was feasible over the desired mission times. Since the problem addressed here involves sequential tests, repeated solution of the resulting semi-Markovian models over mission times of interest is not feasible. Also, as pointed out earlier, the overall system reliability alone may not reflect the true performance of the fault tolerant system because it does not reflect the ill effects of decision delays. This motivates us to examine other cost functions that better reflect the system performance and yield computationally tractable optimization problems for threshold determination. Among such cost functions are those considered in the remainder of this section. They are based upon examination of first passage time properties and duration statistics for semi-Markov chains.

First Passage Times

A semi-Markov chain with N states is completely characterized by an embedded transition probability matrix $[p_{ij}]$ and N^2 conditional holding time pmfs $h_{ij}(m)$ (Howard, 1971). The semi-Markov model can also be completely characterized by defining the transition mass functions $g_{ij}(m)$ defined as,

$$g_{ij}(m) = p_{ij}\, h_{ij}(m) \qquad (1)$$

The transition mass functions $g_{ij}(m)$ have the following property:

$$\sum_{n=1}^{\infty} \sum_{j=1}^{N} g_{ij}(n) = 1 \qquad (2)$$

Equation (2) implies that for fixed i, if we maximize (or minimize) the cumulative sum of the transition mass function for a particular destination state j, then the collective sum of the cumulative sums of the transition mass functions for transitions from state i to all other j is minimized (or maximized). In other words, we will not be able to maximize (or minimize) any one of the transition mass functions independently of the others. This property will be used frequently in deriving the approximate optimal threshold determination method.

The characterization of the system behavior by the $g_{ij}(m)$ allows us to

generate any statistic of interest from the semi-Markov model. One such statistic is the pmf $f_{ij}(n)$ for the time to first passage from state i to state j. This is the probability that the first entrance to state j will occur n time samples after entering state i, and is given by,

$$f_{ij}(n) = g_{ij}(n) + \sum_{\substack{r=1 \\ r\neq j}}^{N} \sum_{m=1}^{n} g_{ir}(m)\, f_{rj}(n-m) \qquad (3)$$

with initial condition $f_{ij}(0)=\delta_{ij}$. The cumulative pmf that the first passage from i to j will require n time samples or less is then given by,

$$F_{ij}(n) = \sum_{k=1}^{n} f_{ij}(k)$$

$$= \sum_{k=1}^{n} g_{ij}(k) + \sum_{k=1}^{n} \sum_{\substack{r=1 \\ r\neq j}}^{N} \sum_{m=1}^{n} g_{ir}(m)\, f_{rj}(k-m) \qquad (4)$$

The first passage time statistics given by (3) or (4) are indicative of the length of time required to make a transition from state i to state j for a semi-Markov chain. A cost function based on these statistics is well suited for our objective, because we would like to minimize the transition time from certain degraded states to more desirable states in the system state description. Thus, a cost function based on first passage times can be representative of the performance degradation for the system during the mission.

We will now illustrate the use of first passage time statistics to establish the thresholds for the SRDTs and SPRTs used in the example system described in the preceding section.

Let us consider State 6 in our model of the quadraplex system given in the preceding section. This state represents a degraded mode of system operation, namely a missed detection at the four-level. We would like to transition out of this state to a more desirable state as quickly as possible. Examining the other states in our model, we notice that State 7 represents the case where the SRDT has correctly detected the presence of a failure. Therefore, we would like to minimize the time for first passage from State 6 to State 7. This can be achieved by maximizing the first passage time cumulative pmf for some fixed n for States 6 & 7, i.e.

$$\text{Max } F_{67}(n) = \text{Max} \sum_{k=1}^{n} f_{67}(k)$$

$$= \text{Max}\left[\sum_{k=1}^{n} g_{67}(k) + \sum_{k=1}^{n} \sum_{\substack{r=1 \\ r\neq 7}}^{N} \sum_{m=1}^{n} g_{6r}(m)\, f_{r7}(k-m) \right] \qquad (5)$$

From Fig. 1, we see that the only way of making a transition to State 7 from State 6 is by a direct transition, which corresponds to detection by the appropriate SRDT of the previously undetected failure. Therefore, the second term in brackets in equation (5) contributes only through the term involving $g_{66}(\cdot)$. Since the recursion in evaluating the convolution term starts with $f_{67}(0)=0$, and noting the relationship among the transition mass functions given by (2), the cumulative pmf $F_{67}(n)$ can be maximized by optimizing the cost function,

$$J_1 = \text{Max} \sum_{k=1}^{n} g_{67}(k) \qquad (6)$$

Because the above cost function represents the probability of an SRDT detection given the presence of one failure, it is characterized completely by the SRDT threshold. Therefore, an unconstrained maximization of (6) would result in an optimal SRDT threshold of zero, and an intolerable number of false detections would result. This is unacceptable.

A lower bound for the SRDT threshold can be established by considering other transitions that are influenced by the threshold that are undesirable. For instance, consider transitions from State 1 to State 2 in the semi-Markov model of the example system. This transition represents a false failure decision by the SRDTs, therefore we would like to maximize the first passage time for this transition. Stated differently, we would like to minimize the cumulative pmf for first passage from State 1 to State 2. That is,

$$\text{Min } F_{12}(n) = \text{Min} \sum_{k=1}^{n} f_{12}(k)$$

$$= \text{Min}\left[\sum_{k=1}^{n} g_{12}(k) + \sum_{k=1}^{n} \sum_{\substack{r=1 \\ r\neq 2}}^{N} \sum_{m=1}^{n} g_{1r}(m)\, f_{r2}(k-m) \right] \qquad (7)$$

The only way of making a transition from state 1 to State 2 is by a direct transition. Neglecting $g_{11}(\cdot)$ for similar reasons to those used in deriving (6), (7) reduces to,

$$J_2 = \text{Min} \sum_{k=1}^{n} g_{12}(k) \qquad (8)$$

An unconstrained minimization of (8) would result in an infinite magnitude for the SRDT threshold. However, (6) and (8) represent cost functions for conflicting objectives. In some sense then, the SRDT threshold can be optimized by defining a performance measure that combines them, such as:

$$\text{Min } \mathcal{F}_1 = \text{Min}\left[\sum_{k=1}^{n} g_{12}(k) - \sum_{k=1}^{n} g_{67}(k) \right] \qquad (9)$$

The time index n appearing in the cost function is arbitrary and can be

selected by the designer. Typically, it should approximate the maximum permissible delay in detecting failures of the mimimum bias magnitude a that cannot be tolerated. It can also depend on the number of instruments in use.

Proceeding along similar lines and using the dependence among the transition mass functions defined by (2), we can show easily that when three instruments are in use, the analogous "optimum" threshold for the SRDT can be obtained by optimizing the cost function

$$\text{Min } \mathcal{F}_2 = \text{Min}\left[\sum_{k=1}^{n} g_{34}(k) - \sum_{k=1}^{n} g_{17,20}(k)\right] \qquad (10)$$

In our example system, the SPRTs are in operation once a detection decision is made by one of the SRDTs. Since the SPRT is a binary hypothesis test, we need to establish two thresholds for each SPRT. Let us consider first fixing the lower threshold A for the SPRT, the crossing of which represents a no failure decision.

In Fig. 1, State 2 represents the presence of a false detection by one of the SRDTs. In this case, we would like the SPRTs to arrive at no failure decisions as quickly as possible so that a desirable transition from State 2 to State 1 occurs. Since we want to minimize the decision delay for this desirable transition, we try to minimize the time for first passage from State 2 to State 1. Again, taking into account the dependence among the transition mass functions for exits from a given state (equation (2)), the first passage time from State 2 to State 1 can be minimized by optimizing the cost function,

$$J_3 = \text{Max} \sum_{k=1}^{n} g_{21}(k) \qquad (11)$$

Assuming that the upper threshold B is fixed, (11) can be maximized by raising the lower threshold A. As before, optimization of the cost function (11) would lead to a lower SPRT threshold that produced an unacceptable rate of incorrect no failure decisions. To avoid this, an upper bound for A is obtained by considering transitions from State 7 to State 6 at the four-level stage. This transition occurs when the SPRTs fail to isolate a faulty instrument. In order to minimize the likelihood of this decision error, we minimize the cumulative pmf for the first passage time from State 7 to State 6, the general form of which is given by (4). This can be achieved by optimizing:

$$J_4 = \text{Min} \sum_{K=1}^{n} g_{76}(k) \qquad (12)$$

The conflicting objectives defined by (11) and (12) can be combined into a single cost function

$$\text{Min } \mathcal{F}_3 = \text{Min}\left[\sum_{k=1}^{n} g_{76}(k) - \sum_{k=1}^{n} g_{21}(k)\right] \qquad (13)$$

Minimization of the cost function (13) for a fixed value of B will give the optimum lower threshold A for the SPRTs.

Proceeding in an analogous manner, the optimal SPRT upper threshold B at the four-level stage can be derived by optimizing a cost function

$$\text{Min } \mathcal{F}_4 = \text{Min}\left[\sum_{k=1}^{n} g_{23}(k) - \sum_{k=1}^{n} g_{7,10}(k)\right] \qquad (14)$$

Again, the index n is to be picked by the designer depending on the maximum permissible delay for the minimum intolerable failure bias before an instrument must be isolated.

Duration

The motivation behind selecting optimal thresholds by the methods described above is to minimize the time spent in degraded modes of system operation while maximizing the time spent in healthy states. Here, healthy states imply all unfailed components are in use with no detection decisions by the sequential tests. By examining the duration statistics for each state, we will show in this section that the optimization of the cost functions defined above will in fact achieve these objectives.

Duration of a state is defined as the length of time a state is occupied following its entrance until a transition occurs to some state other than itself. The pmf for the duration in state i is given by,

$$d_i(n) = \sum_{\substack{j=1 \\ j \neq i}}^{N} g_{ij}(n) + \sum_{m=1}^{n} g_{ii}(m)\, d_i(n-m) \qquad (15)$$

with the initial conditions $d_i(0)=0$. The cumulative pmf for the duration in a state (i.e. the probability that the duration is less than or equal to n samples) is given by,

$$D_i(n) = \sum_{k=1}^{n} d_i(k)$$

$$= \sum_{k=1}^{n} \sum_{\substack{j=1 \\ j \neq i}}^{N} g_{ij}(n) + \sum_{k=1}^{n} \sum_{m=1}^{n} g_{ii}(m)\, d_i(n-m) \qquad (16)$$

To minimize the probability that the duration exceeds n samples in a state i, we have to maximize the cumulative pmf $D_i(n)$ given by (16), and vice versa. Further, we would like to achieve this by optimizing the threshold for the sequential test. This in turn implies that the optimization has to be restricted to those transitions which depend explicitly on the test threshold being optimized.

Consider State 6 in the evaluation model of the example system. This represents a degraded state due to the presence of an undetected failure. Hence, we would like to minimize the duration in this state by selecting the threshold for the SRDT. Since the transition mass function $g_{67}(n)$ is an explicit function of the SRDT threshold, we can minimize the probability that the duration exceeds n samples in State 6 as a function of the SRDT threshold by defining the cost function as:

$$J_5 = \text{Min} \sum_{k=1}^{n} g_{67}(k) \qquad (17)$$

The constraint on (17) is the requirement to keep false alarms by the SRDTs low, which in turn implies the probability that the duration of State 1 exceeds n should be maximized. Combination of these two conflicting objectives leads to a cost function identical to (9).

We know that first passage time is a measure of the time needed to reach a given state from another state, while duration measures the time needed to leave a given state. We infer from this section that optimization of the performance measures defined earlier minimizes the duration in the degraded system states, while first passage time considerations guarantee that this is achieved through desirable transitions in the model. In other words, the selected thresholds guarantee quick failure detection and isolation while at the same time reducing to the greatest extent possible the number of false alarms.

NUMERICAL RESULTS

The optimum threshold determination technique described above was applied to the quadraplex redundant sensor system with the FDI logic structure discussed previously. It is assumed for the calculations that the FDI logic operates at a rate of 1 Hz and that the failure rate per time step of each instrument is $\varepsilon=5\times10^{-7}$ (which corresponds to a mean time to failure of 556 hours). An upper limit of 25 secs for the SRDTs to detect the minimum intolerable failure bias magnitude α is also assumed. Identical assumptions were made for the SPRTs used to isolate the first and second failures. This results in setting n=25 in the cost functions defined above.

In general, the cost functions developed above are functions of the component failure rate ε, the minimum failure bias magnitude α, the variance σ^2 of the residual sequence $\{r_k\}$, the assumed maximum decision delay time index n, and the failure detection test thresholds. Assuming that all parameters other than the test thresholds are fixed, the cost functions can be optimized by a suitable choice of the test thresholds. Interestingly, the cost functions defined above are all convex in the thresholds for this example, hence they yield unique optimal thresholds. This convexity of the cost functions cannot be assumed for all problems, but a convex hull can always be defined because the cost functions always become monotonic as the threshold approaches its limiting values.

To illustrate the cost convexity for the example system, the cost functions defined above for the selecting the SRDT and SPRT upper thresholds are plotted as functions of the test thresholds in Figs. 3 and 4, respectively. A relatively simple golden section search can be used to find the optimum thresholds in this case. For the SPRT, since two thresholds must be determined, a few iterations are required to arrive at the optimal thresholds A^* and B^* after an initial guess is made for A and B. In all cases, the iterations converged to two decimal place accuracy in about 25-30 secs of CPU time on a VAX 6240.

Table 1 shows the cost function values and optimum threshold for the SRDT at the 4-level stage as a function of the minimum failure bias α, the noise level σ and the maximum allowable detection time n. Also tabulated are the average time to detect failures (ATDF) by the SRDTs for the cases examined.

The ATDF is calculated from,

$$ATDF = \lim_{m \to \infty} \sum_{k=1}^{m} k\, g_{67}(k) / \sum_{k=1}^{m} g_{67}(k) \qquad (18)$$

Since the $g_{ij}(k)$ that appears in (18) has negligible probability mass for large k, an upper limit of m=100 was sufficient to calculate the ATDF for the example considered here.

Many interesting conclusions can be drawn from the SRDT results. Note that as the minimum failure bias level to be detected increases for a fixed noise level σ, the cost function value approaches the limiting value of one. If, on the other hand, the failure bias a decreases for fixed σ, then the optimum cost function value drops considerably below one. In fact, the cost function value can be regarded as a figure of merit for the FDI performance. A value considerably lower than one for this implies that the FDI scheme is prone to false alarms.

The ATDF is also a useful performance measure for the test designer. It indicates the average time delay in detecting a failure by the SRDTs for the chosen maximum delay time index n. We notice that it approaches the upper limit n=25 as the figure of merit value decreases.

If the maximum delay time index n is increased from 25 to 50 for identical values of a and σ, the SRDT figure of merit improves but at the cost of increased ATDF. This implies that the FDI scheme can take more time to arrive at failure decisions, the net effect of which is increased threshold levels that reduce the number of false decisions. Note the very high value of the figure of merit in this case.

With the optimum cost function value and the ATDF at hand, the designer can make the trade-off between false alarm rate and speed of detection in designing the SRDT. The authors' experience has been that a cost function value below 0.9 usually results in an unacceptable false alarm rate (on the order of 10^{-2} to 10^{-1} per test). Under these circumstances, the designer must either increase the permissible time to detection or increase the minimum failure bias level in order to arrive at an acceptable trade-off.

The SPRT cost functions developed above exhibited identical characteristics when applied to the example system and are omitted here for conciseness. We

point out that at both the 3-level and the 4-level stage, the optimum SPRT thresholds were found to be $A^*=-3.33$ and $B^*=4.49$ for the case $a=\sigma=1.0$ and $n=25$. We note in passing that for the SPRT at the 4-level, the transition mass function $g_{7,10}(\cdot)$ needs to be used in (18) to define the ATDF. The ATDF using the threshold values given was 11.79.

Particularly in the case of the SPRT thresholds just considered, we note that the threshold level for deciding H_1 is considerably higher than the 3σ level. For the above values of A^* and B^*, the per-test error probabilities for the SPRT are: $P_{fa}=0.011$ and $P_m=0.035$. When Walker and Gai (1979) minimized the cost function P_{SL}, their threshold produced a miss probability of $P_m=0.999$ during most of the mission time. It is clear, as pointed out by Walker and Gai (1979) that the cost function they considered includes no mechanism for dealing with the elapsed time between the onset and detection of a failure, which tends to result in thresholds that delay the FDI decisions until the last subinterval of the mission.

To examine the overall performance of the example fault tolerant system for the thresholds generated here, the semi-Markov model was used to generate the state probabilities for a mission length of just over an hour (actually, 4000 secs). From this, the probability of occupying the system loss state at the end of the mission can be determined. Note that this evaluation is *not* necessary to determine the thresholds, as it was for Walker and Gai (1979). The results are presented in Table 2 under case (1) for various threshold combinations when $a=\sigma=1$. In generating the results, it is assumed that the pmfs are truncated after 100 time steps for computational tractability. It is also assumed that the BITE which operates on isolated instruments has a probability of making a false failure decision on an unfailed instrument per test (P_0) of 0.2 and a probability of a no failure decision on a failed instrument per test (P_1) of 0.4. BITE is assumed to operate at a rate of 0.5 Hz.

We notice that P_{SL} decreases as the threshold levels increase. This reflects the lack of penalization of an undetected failure that permits delayed decisions in favor of decreased false alarm rates when P_{SL} is used as the cost function. Since there is no mechanism to penalize such delayed decisions, minimization of P_{SL} alone will produce miss probabilities close to one, as obtained by Walker and Gai (1979). We notice also that the system

loss probability for the use of 3σ as the thresholds is very high relative to P_{SL} for the optimal thresholds.

To examine the FDI performance in terms of minimizing the duration in the degraded states, the semi-Markov model described above was modified to penalize delayed FDI decisions. This was done by adding to the model direct transitions from all states involving a delayed decision to the system loss state if the failure is undetected for 25 secs. Thus, a hard upper limit of 25 secs is enforced for the SRDT and SPRT to reach failure decisions in the presence of a failure. The results for this modified system model are tabulated as case (2) in Table 2. All numerical parameters were the same as the previous case. Here, it is assumed that $P_0=0.2$ and $P_1=0.3$. For this case, we notice that as the threshold level increases, the system loss probability P_{SL} increases, which is contrary to the results in case (1) examined above. We also notice that the system loss probability values are substantially larger (by 2 orders of magnitude) than the previous results, reflecting a heavy penalty for delayed FDI decisions.

CONCLUDING REMARKS

From the results for the two models presented in Table 2, it is clear that a cost function that uses P_{SL} alone as the criterion for deriving optimum test thresholds does not reflect the performance degradation suffered during the mission due to delays in detecting failures. This is because penalization of undetected failures is difficult to include in such cost functions. Also, it took nearly 6 hours CPU time on a VAX 6240 to calculate P_{SL} for each case examined above. For longer mission lengths, or in cases where the FDI logic operates at a faster rate, it is clearly not feasible to repeatedly solve the semi-Markov model numerically to examine the state probability behavior as thresholds are varied. Instead, use of simpler cost functions based on a few key transitions, as was done here, yields approximately optimal thresholds by relatively simple computations.

It can be easily verified that the ASN for the various cases examined in Table 1 are widely different, even though the ATDFs are fairly close to each other. Therefore, ASN information on the individual tests is not necessarily meaningful for selecting the thresholds.

Notice also that the construction of the complete semi-Markov model for the fault tolerant system is not necessary to construct the cost functions considered here. The designer needs to derive only the transition mass functions appearing in the cost in order to derive the optimum thresholds.

The technique presented in this paper solves the problem of optimum threshold selection for sequential FDI tests in a computationally efficient way. The cost functions to be optimized are relatively easy to develop and do not require the complete construction of the semi-Markov system reliability model. Accounting for time varying noise statistics is relatively simple. Also, the overall fault tolerant system performance is closely correlated with the figure of merit and ATDF for the selected thresholds.

ACKNOWLEDGMENT

This work was supported in part by the Air Force Office of Scientific Research under grants AFOSR-88-0131 and AFOSR-89-0486.

REFERENCES

Bhate, D.H. (1959). Approximation to the distribution of sample size for sequential tests, Biometrika, 46, pp. 130-138.

Gai, E., Harrison, J.V., and Deyst, J.J. (1981). Availability analysis of a redundant data collection and display system for nuclear power plants, Proc. of American Control Conf. (Charlottesville, Virginia), IEEE, New York.

Harrison, J.V., Daly, K.C., Gai, E., Adams, M., and Ginter, S.D. (1979). Navigation performance of an aided redundant strapdown IMU in normal and failure modes, Proc. of AIAA Guid. and Control Conf. (Boulder, Colorado), AIAA, New York.

Howard, R.A. (1971). Dynamic Probabilistic Systems, Volume II: Semi-Markov and Decision Processes, Wiley, New York.

Howell, W., Bundick, T., Hueschen, R., and Ostroff, A. (1983). Restructurable controls for aircraft, Proc. of AIAA Guid. and Control Conf.

(Gatlinburg, Tennessee), AIAA, New York.

Kerr, T. (1987). Decentralized filtering and redundancy management for multisensor navigation, IEEE Trans. on Aerospace and Electronic Sys., AES-23, 1, 83-119.

Looze, D., Weiss, J., Eterno, J., and Barrett, N. (1985). An automatic redesign procedure for restructurable control systems, IEEE Control Systems Mag., vol. 5, no. 2, pp. 16-22.

Moerder, D.D., Halyo, N., Broussard, J., and Caglayan, A.K. (1989). Application of precomputed control laws in a reconfigurable aircraft flight control system, J. Guid., Control and Dyn., vol. 12, no.3, pp. 325-333.

Page, E.S. (1954). Continuous inspection schemes, Biometrika, vol. 41, pp. 100-115.

Srichander, R. (1990). Fault tolerant control of continuous time systems, Ph.D. thesis, Dept. of Aerospace Eng. and Eng. Mechanics, Univ. of Cincinnati, Cincinnati.

Srichander, R., Walker, B.K. (1989). An approximate algorithm for evaluation of semi-Markov reliability models, Proc. of American Control Conf. (Pittsburgh), IEEE, New York.

Wald, A. (1947). Sequential Analysis, Wiley, New York.

Walker, B.K. (1980). A semi-Markov approach to quantifying fault-tolerant system performance, Sc.D. thesis, Dept. of Aero. & Astro., Mass. Inst. of Techn., Cambridge, Mass.

Walker, B.K., Chu, S.K., Wereley, N. (1988). Approximate evaluation of reliability and availability via perturbation analysis, final technical report on Grant AFOSR-84-0160, Dept. of Aerospace Eng. & Eng. Mech., Univ. of Cincinnati, Cincinnati.

Walker, B.K., and Gai, E. (1979). Fault detection threshold determination technique using Markov theory, J. Guid., Control, & Dyn., 2, 4, pp. 313-319.

Wereley, N. (1987). An approximate method for evaluating generalized Markov chain reliability models of fault tolerant systems, M.S. thesis, Dept. of Aero. and Astro., Mass. Inst. of Techn., Cambridge, Mass.

Willsky, A.S. (1976). A survey of design methods for failure detection in dynamic systems, Automatica, vol. 12, no. 6, pp. 601-611.

Table 1 SRDT thresholds and performance for various cases

No.	n	a	σ	B1	$\mathcal{F}_1$	ATDF
1	25	0.8	1.0	6.32	0.8287	15.53
2	25	1.0	1.0	6.21	0.9344	12.77
3	25	1.2	1.0	6.18	0.9809	10.90
4	25	1.0	1.2	7.56	0.8517	14.99
5	25	1.0	0.8	4.94	0.9586	10.50
6	25	0.8	1.2	7.78	0.7093	18.22
7	50	1.0	1.0	8.59	0.9967	17.55

Table 2 Comparison of system loss probabilities

case	B1	A	B	P_{sl}
1	3.0	-3.0	3.0	0.51982×10^{-3}
1	5.0	-3.67	4.83	0.11508×10^{-4}
1	6.2	-3.67	4.83	0.22663×10^{-5}
1	6.6	-3.67	4.83	0.14447×10^{-5}
1*	6.2	-3.33	4.49	0.24947×10^{-5}
2	5.0	-3.67	4.83	0.67409×10^{-3}
2	6.2	-3.67	4.83	0.78355×10^{-3}
2	6.6	-3.67	4.83	0.85756×10^{-3}
2*	6.2	-3.33	4.49	0.69485×10^{-3}

* designates the use of optimal thresholds for this case

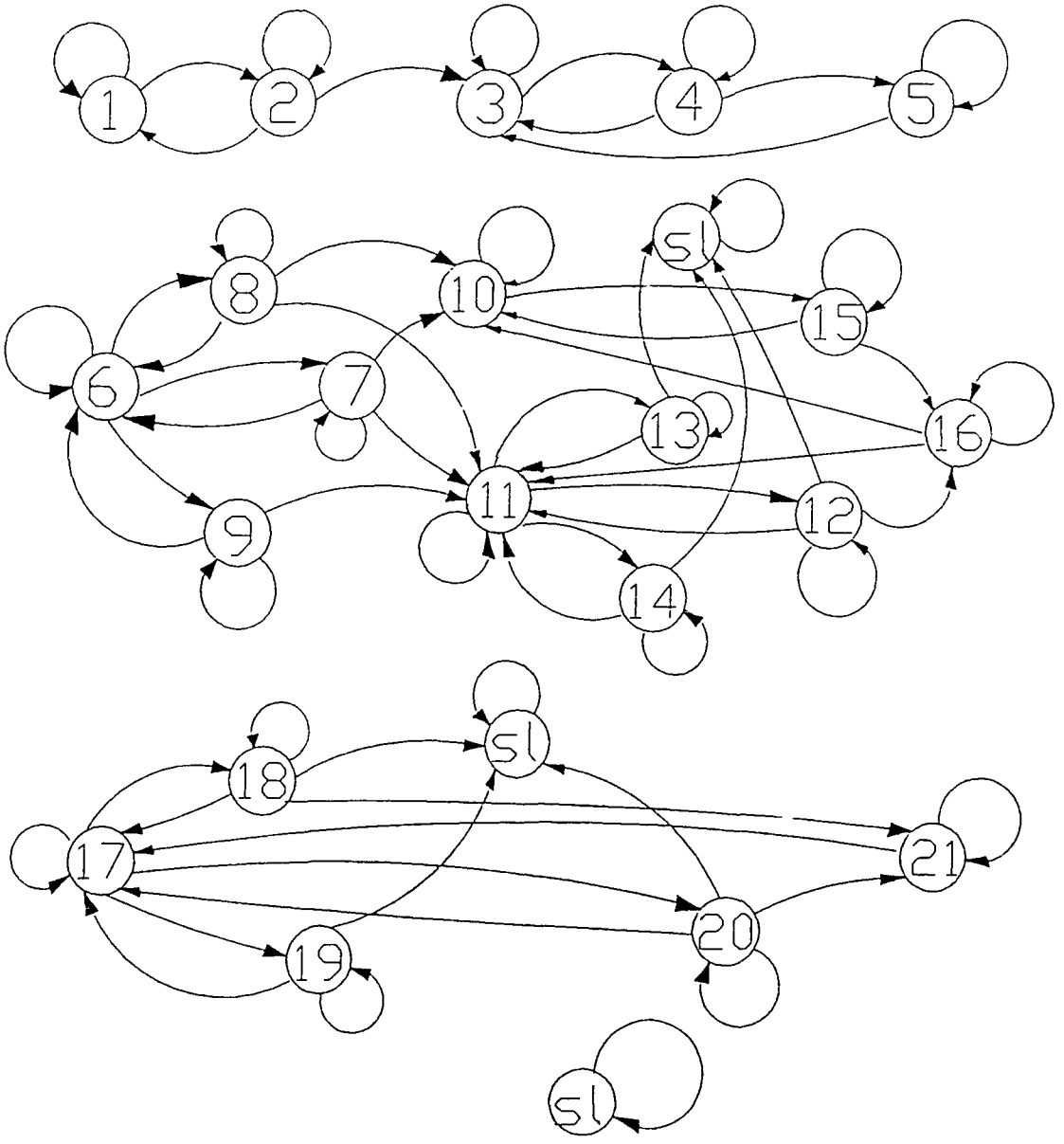
Captions for Figures

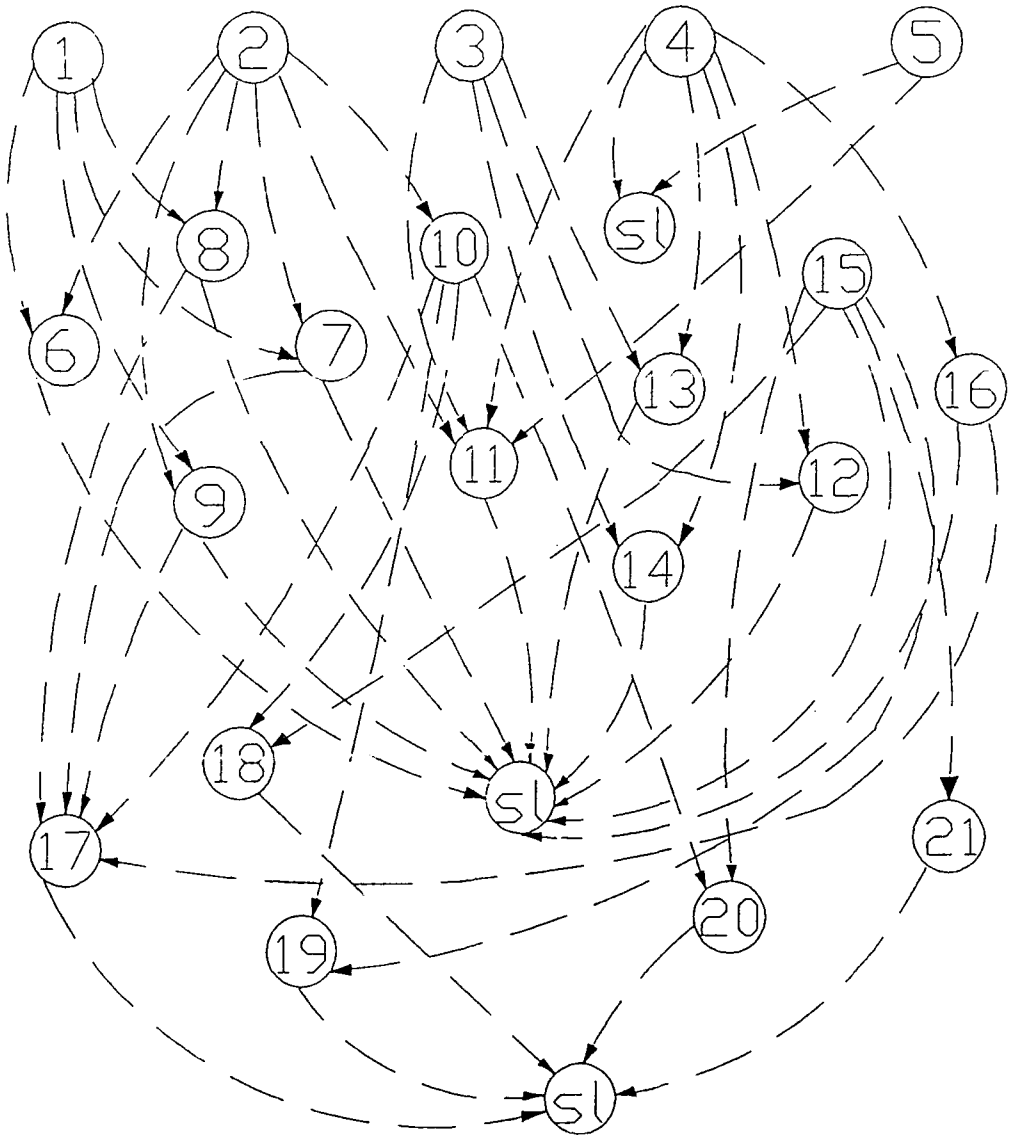
Fig. 1 FDI rate dependent state transition diagram for semi-Markov model.

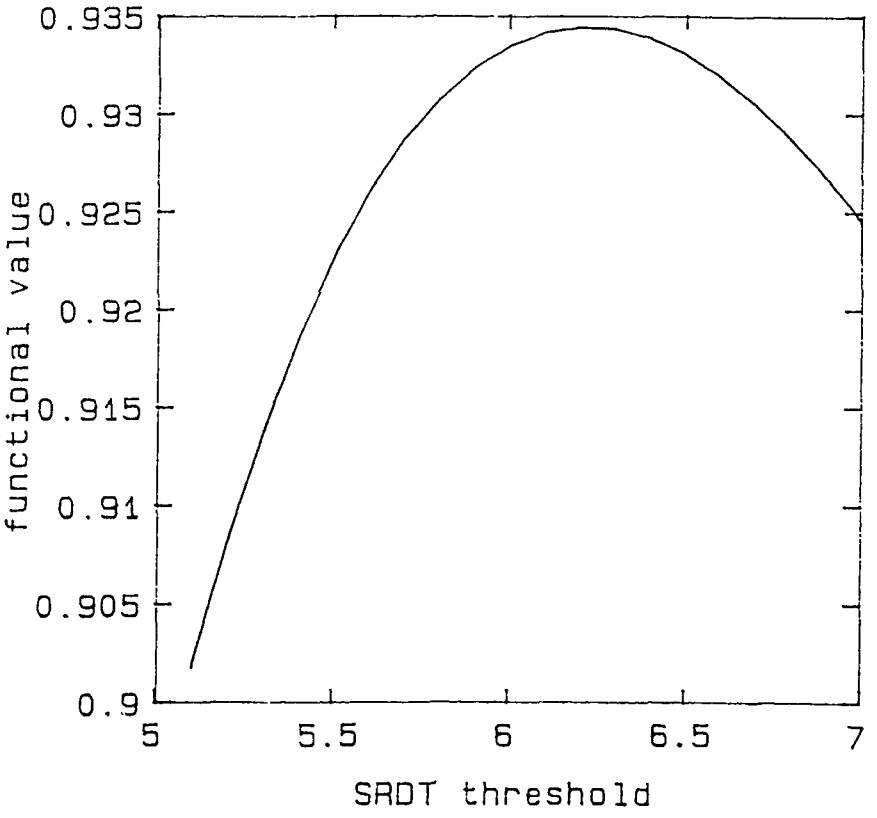
Fig. 2 Failure rate dependent state transition diagram for semi-Markov model.

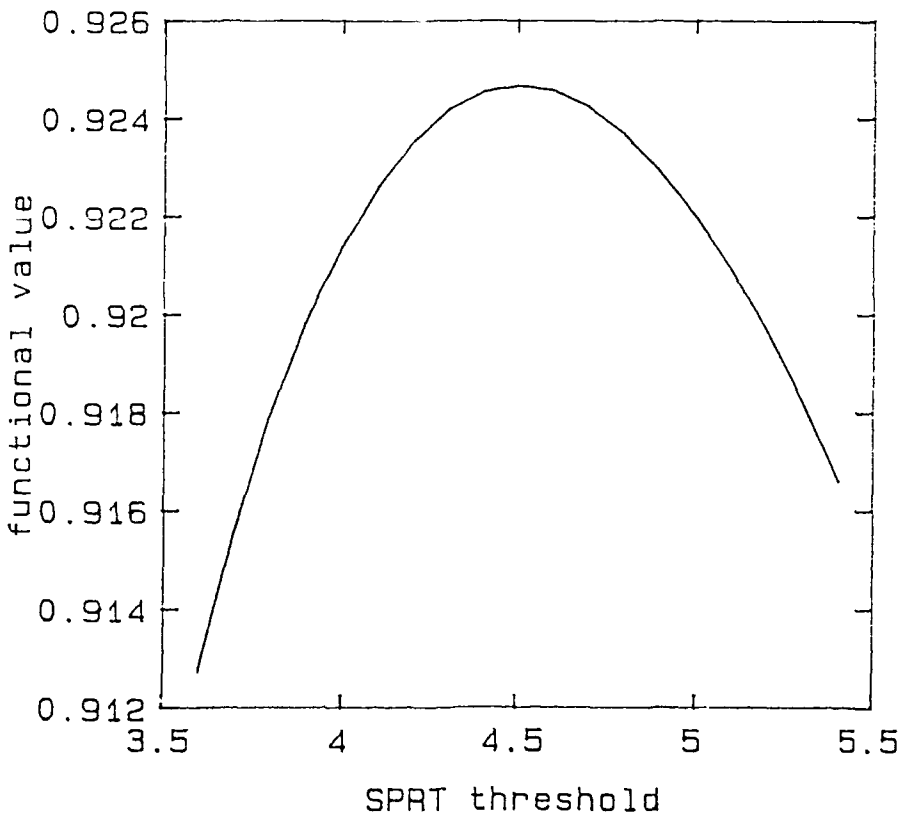
Fig. 3 SRDT threshold versus cost function value.

Fig. 4 SPRT upper threshold versus cost function value.


1
2
3
4
5
sl
8
10
15
6
7
13
16
11
12
9
14
sl
18
17
21
20
19
sl


1
2
3
4
5
8
10
sl
15
6
7
13
16
11
12
9
14
18
sl
17
21
20
19
sl


0.935
0.93
0.925
0.92
0.915
0.91
0.905
0.9
functional value
5
5.5
6
6.5
7
SRDT threshold


0.926
0.924
0.922
0.92
0.918
0.916
0.914
0.912
functional value
3.5
4
4.5
5
5.5
SPRT threshold

2.2 Stochastic Stability Tests for FTCS

One of the key issues in FTCS analysis is the determination of the stability of the system, particularly when the system uses feedback control that is reconfigured in response to the FDI decisions Only recently have the results of stochastic stability analysis been applied to FTCS. To date, these results were restricted to FTCS for which the FDI decisions are always correct, though possibly delayed by either one time sample or by a random number of time samples [11,12]. Our stability results, which are reported in the manuscript that follows, are not restricted to this case. Furthermore, for the special case of LTI FTCS with linear state feedback control, we derive necessary and sufficient conditions for a relatively strong form of stochastic stability, whereas all of the conditions that have been derived previously are only sufficient.

STOCHASTIC STABILITY ANALYSIS FOR CONTINUOUS TIME FAULT TOLERANT CONTROL SYSTEMS

by

R. Srichander
Graduate Research Assistant

&

Bruce K. Walker
Associate Professor

Department of Aerospace Engineering
& Engineering Mechanics
Mail Location 343
University of Cincinnati
Cincinnati, OH 45221-0343
Tel: (513) 556-3552
FAX: (513) 556-4589

ABSTRACT

Active fault tolerant control systems are feedback control systems that reconfigure the control law in real time based on the response from an automatic failure detection and identification (FDI) scheme. The dynamic behavior of such systems is characterized by stochastic differential equations because of the random nature of the failure events and the FDI decisions. The stability analysis of these systems is addressed in this paper using stochastic Lyapunov functions and supermartingale theorems. Both exponential stability in the mean square and almost sure asymptotic stability in probability are addressed. In particular, for linear systems where the coefficients of the closed loop system dynamics are functions of two random processes with Markovian transition characteristics (one representing the random failures and the other representing the FDI decision behavior), necessary and sufficient conditions for exponential stability in the mean square are developed.

1. INTRODUCTION

Fault tolerant control systems have been developed in order to achieve high levels of reliability and performance in situations where the controlled system can have potentially damaging effects on the environment when failures of its components take place. For instance, in hazardous chemical and nuclear plants, the consequences of an improper control action following a control system component failure can be disastrous. In fighter aircraft, the desire for increased maneuverability and performance has led to relaxation of the static stability requirements. The failure of a flight control element in such cases can result in an unstable aircraft if the system design does not properly account for it. In the case of manned space systems, safety is the greatest priority, which implies that even in the presence of failed components the spacecraft must be able to return safely to its base. Other high performance automatic system applications where reliability is of prime importance include air traffic control systems, computerized banking systems and automatic medical monitoring systems.

A fault tolerant control system is designed to retain some portion of its control integrity in the event of a specified set of possible component failures or large changes in the system operating conditions that resemble these failures. Fault tolerant control system designs can be broadly classified into two categories: passive designs and active designs. Each will be described below.

A passive fault tolerant control system can tolerate one or more component failures while satisfactorily accomplishing its mission without reconfiguring itself. Among sensing systems, for instance, the passive fault tolerant design category includes those systems that incorporate a mid-value measurement selection strategy (Potter and Suman 1986) or an averaging strategy for generating the outputs of redundant sensors. Various degrees of passive fault tolerance can also be achieved through such techniques as robust control design (where "robust" refers here to insensitivity to the effects of failures) or simultaneous actuation by parallel controllers (Petkovski 1987, Vidyasagar and Vishwanadham 1985, Yedavalli 1985).

Active fault tolerance, on the other hand, involves automatically detecting and identifying the failed components (Patton *et al.* 1989, Walker 1983, Willsky 1976, Willsky and Jones 1976) and then reconfiguring the control law on-line in response to these decisions. Several examples of

active fault tolerant control system designs have appeared in the literature recently, primarily for reconfigurable control of tactical aircraft (Caglayan *et al.* 1987, Howell *et al.* 1983, Looze *et al.* 1984, Looze *et al.* 1985, Moerder *et al.* 1989).

In this paper, we will be concerned with control systems that have automatic failure monitoring capability in order to reorganize or reconfigure the control law in real time in response to failure indications. In other words, we will consider the behavior of active fault tolerant control systems. In particular, we will consider the closed loop stability of active fault tolerant control systems when the random events that affect these systems, namely component failures and failure detection decisions, are taken into account.

The dynamic behavior of active fault tolerant control systems is governed by stochastic differential equations because the failures and failure detection decisions occur randomly. Stochastic differential equations arise in a variety of problems of practical interest. In structural engineering, for instance, the study of the dynamic stability of elastic structural and mechanical systems subjected to randomly fluctuating loads generate these equations. In communications engineering, tracking noise in a radar system leads to Itô differential equations describing the dynamics of a moving target. For the control engineer, random perturbations acting on the controlled process generate equations of the Itô type describing the dynamic behavior of the system. The study of the scattering phenomenon in random media and other chemical and biological problems also generate governing equations with stochastic coefficients. Many other examples of stochastic differential equations in engineering systems can be cited.

In this paper, the stability analysis of active fault tolerant control systems leads to the study of differential equations with randomly varying parameters. Using techniques from the theory of stochastic differential equations, the stability analysis of these systems will be presented here. The synthesis of fault tolerant control laws for these systems is another important issue. This will be discussed in a companion paper (Srichander and Walker, 1990).

As pointed out above, the dynamical behavior of fault tolerant control systems is governed by stochastic differential equations. Of primary interest in this paper is the stability of the solutions to these stochastic

differential equations. Several authors have examined the stability of solutions to general stochastic differential equations (Bertram and Sarachick 1959, Bucy 1965, Kats and Krasovskii 1960, Khasminskii 1967, Khasminskii 1980, Kozin 1969, Kozin 1972, Kushner 1967, Kushner 1971). Existing stability results can be broadly characterized as applying to two categories of stochastic differential equations. One category is stochastic differential equations perturbed by Gaussian white noise (Itô differential equations). The other is stochastic differential equations whose coefficients vary randomly with Markovian characteristics. Of these categories, the advances in the study of stability of solutions to Itô differential equations have been more significant. This is true primarily because the solutions to Itô differential equations are Markov diffusion processes, which can be constructed using a Picard iteration technique to solve the associated stochastic integral equation. For a rigorous analysis of the existence, uniqueness, and behavior of the solutions to Itô differential equations, we refer the reader to (Khasminskii 1962, Khasminskii 1967, Khasminskii 1980, Nevelson 1966).

For differential equations with random Markovian coefficients, significant results were obtained by Bucy (1965), Kats and Krasovskii (1960), and Kushner (1967). In the work of Kats and Krasovskii (1960), the stability of the moments of the solution process is investigated in detail using a stochastic Lyapunov function approach. Kushner (1967, 1972) and Bucy (1965) employ the supermartingale property of stochastic Lyapunov functions to study the stability of the sample paths of the solutions. This is very significant in practical problems of interest because, for a real system in operation, we will observe only a single sample solution. Hence, the stability results of the most practical importance are those that guarantee the stability of every sample solution of the stochastic system, as opposed to results on the stability of the moments of the sample solutions.

The stochastic description of fault tolerant control system behavior studied in this paper differs from the stochastic systems investigated in the literature cited above. For the systems considered here, the random variations occurring in the system description are modeled as failures with Markovian transition characteristics, and this leads to a stochastic differential equation description of standard form. However, there is an additional random process that induces random variations in the control law, and therefore further affects the system description. This additional random

process is the failure detection and identification (FDI) process, which changes the system description through the control reconfiguration strategy.

For linear fault tolerant control systems with instantaneous detection of the transitions of the failure process by the FDI process assumed, the minimization of a quadratic cost function leads to the jump linear quadratic regulator (JLQR) formulation investigated by Wonham (1971) and Sworder (1969). The instantaneous detection assumption is very restrictive, however, and renders these results invalid for many fault tolerant systems of practical interest.

More recently, the stability of active fault tolerant linear control systems with possible detection delays was investigated by Mariton (1989) under the assumption of identical state spaces for the failure process and the FDI process. The probability of false alarms is also accounted for in deriving these stability results. Mariton uses quadratic stochastic Lyapunov function candidates to derive *sufficient* conditions for exponential stability in the mean square of the closed loop system. However, in deriving these results, Mariton (1989) assumes that a correct failure diagnosis is always made following a failure subject only to a random time delay. This assumption is too restrictive for many problems of practical interest where incorrect failure diagnosis is common due to the noisy signal environment. Furthermore, because the conditions derived by Mariton (1989) are sufficient and not necessary, they are inadequate to reach useful stability conclusions when they are violated.

The JLQR problem has been reexamined recently by Ji and Chizeck (1990) in the context of deriving stochastic controllability and stabilizability conditions. In particular, necessary and sufficient conditions for the stabilizability of the Markovian JLQR problem have been derived (though these conditions are difficult to check in practice). As in most of the analyses cited above, however, the restrictive assumption of instantaneous failure detection is assumed in deriving these results.

The inadequacy of the existing results in characterizing the stability of active fault tolerant control systems is the primary motivation behind this paper. Specifically, we will investigate in this paper cases where the FDI decision process is random with Markovian characteristics, such as when memoryless FDI tests are used on measurement data corrupted by additive white noise. In particular, *necessary and sufficient* conditions for the stochastic stability of linear fault tolerant control systems under these

conditions will be derived. These results are derived without the restrictive assumption of identical state spaces for the FDI and failure processes and without the restrictive assumption of instantaneous failure detection, thereby making them applicable to many practical fault tolerant control systems. The basic tools for the stability analysis will be stochastic Lyapunov functions (Kushner 1967) and supermartingale theorems (Doob 1956).

The paper is organized as follows: Section 2 discusses the mathematical formulation of the active fault tolerant control problem for continuous time systems. A brief description of the assumptions regarding the FDI process and the notation used in this paper are also given. In section 3, we will present some useful results on supermartingales and define the notion of stochastic stability. Conditions for the stochastic stability of the general dynamic system defined in section 2 are derived in section 4. These results are applied in section 5 to derive *necessary and sufficient* conditions for the exponential stability in mean square of a linear stochastic dynamic system of the form that fault tolerant control systems take when the failure and FDI processes are Markovian. Section 5 also shows that the JLQR results of (Wonham, 1971) follow as a special case of our results, and that almost sure asymptotic stability in probability is guaranteed when the conditions for exponential stability in mean square are satisfied. Conclusions are then given in section 6.

The results of this paper allow us to unambiguously determine the stochastic stability of active fault tolerant systems with Markovian failure and FDI characteristics, including some of the reconfigurable control strategies that have been presented in the literature. Under certain conditions, these reconfigurable control laws can lead to a closed loop system that does not possess stochastic stability despite the fact that the reconfiguration law always leads to a deterministically stable feedback system. This will be illustrated in the companion paper (Srichander and Walker, 1990) using a numerical example.

2. PROBLEM FORMULATION

In designing active fault tolerant control systems, we are interested in monitoring the random variations that occur in the system description due to random failures in order to change the control accordingly. In practice, these random variations are not directly measurable but rather can only be

monitored by an FDI scheme, which is subject to errors and delays. Let r(t) denote the state of the FDI process which monitors the state $\eta(t)$ of the random process describing the failures. The process r(t) is a finite state stochastic process whose random behavior is conditioned on the failure process state $\eta(t)$. We are interested in designing a control law to generate the system input u(t), such that the control law is a function only of the FDI process state r(t) and the system states x(t), and such that the solution x=0 for the dynamical system,

$$\dot{x}(t) = f(x(t), \eta(t), u(x(t), r(t), t), t) \tag{2.1}$$

is stable $\forall t \geq t_0$. (We assume here without loss of generality that x=0 is a solution to (2.1)). Note that we do *not* allow the control to be a function of the actual failure process state $\eta(t)$.

In the discussion to follow, we assume that $\eta(t)$ and r(t) are separable measurable Markov processes (Doob 1956) with finite state spaces $\mathbf{Z}=\{1,\ldots,\nu\}$ and $\mathbf{S}=\{1,\ldots,\gamma\}$, respectively. Thus, the system description depends upon the true failure state $\eta(t)$ while the input that is applied to the plant depends upon the control law used in response to the indication by the FDI process that the system state is r(t). In real systems, it is often true that $r(t) \neq \eta(t)$, and this will be the starting point for much of the analysis that follows. The stability analysis in section 4 will pertain mostly to the general nonlinear stochastic dynamical system described by (2.1). Later in our stability analysis, we will consider a special case of the system (2.1) whose state space description is of the linear form,

$$\dot{x}(t) = Ax(t) + B(\eta(t))u(x(t), r(t)) \tag{2.2}$$

where, $u(x(t), r(t)) = -K(r(t))x(t)$. Equation (2.2) will be referred to as the *linear plant model* in this paper.

Note that both descriptions above restrict the effects of the random variations due to failures to the input matrix B. This restriction is only for convenience and the nature of the results remains the same when the plant matrix is also subject to random variations.

For notational simplicity, we will denote $B(\eta(t)) = B_k$ when $\eta(t) = k \in \mathbf{Z}$ and $u(x(t), r(t), t) = u_i$ when $r(t) = i \in \mathbf{S}$ wherever appropriate. We also denote x(t)=x,

$r(t)=r$, and $\eta(t)=\eta$ wherever no confusion arises regarding the time dependence of these quantities. We shall assume that the pairs (A,B_k) in (2.2) are controllable for each $k\in Z$. This assumption implies that the given system has redundant control elements, which is a generic property of any fault tolerant system architecture.

The following notations will also be used in the sequel. $\|x\|$ will denote the L^2 norm, i.e. $\|x\|=\left(x_1^2 + x_2^2 +\ldots+ x_n^2\right)^{1/2}$ where x_i are the components of $x\in R^n$. When $t=t_0$, the initial conditions will be denoted by $x(t_0)=x_0$, $r(t_0)= r_0$, $\eta(t_0)= \eta_0$. The inner product of two vectors will be denoted by $\langle\cdot,\cdot\rangle$. The notation $o(\Delta t)$ will denote infinitesimal terms of order strictly higher than one in Δt (i.e. $\lim_{\Delta t\to 0} \frac{o(\Delta t)}{\Delta t} =0$). A positive definite matrix N will be denoted by $N>0$ and a positive semi-definite matrix by $N\geq 0$. We will call a mxn matrix A bounded if there exists a positive constant β such that $\|Ax\|\leq\beta\|x\|$ $\forall x\in R^n$, $x\neq 0$.

We further assume that $f(x,\eta,u(x,r,t),t)$ in (2.1) is a Borel-measurable function of (x,r,η) satisfying the following conditions.

1. There exists a constant L such that if x' and x'' are any two solutions of (2.1) with $\|x'\|$, $\|x''\|<R$, then,

$$|f(x'',\eta,u(x,r,t),t)-f(x',\eta,u(x,r,t),t)| \leq L\|x''-x'\| \qquad (2.3)$$

In (2.3), L is referred to as the global Lipschitz constant in x.

2. The function $f(x,\eta,u(x,r,t),t)$ satisfies,

$$f(0,\eta,u(x,r,t),t) = 0, \ \forall r\in S, \ \forall\eta\in Z, \text{ and } \forall t\geq t_0 \qquad (2.4)$$

Under these conditions, the solution $x(t)=x(t;x_0,r_0,\eta_0,t_0)$ of (2.1) is almost surely unique and is an absolutely continuous stochastic process. (This can be seen following arguments in Khasminskii (1980)). Note that the linear system (2.2) is a special case of $f(\cdot)$ satisfying these conditions.

Further, it can be easily shown that the joint process $\{x,r,\eta\}$ whose realizations satisfy (2.1) is a (n+2)-dimensional Markov process. To see this, let us consider the interval $t_0\leq s\leq t$. Then, x(t) is determined uniquely by x(s) and by $\eta(\tau)$ and $r(\tau)$ for $s\leq\tau\leq t$. Under the assumption that $\eta(t)$ and $r(t)$ are Markov processes, it follows that $\eta(\tau)$ and $r(\tau)$ for $\tau\geq s$ are

independent of $\eta(\tau')$ and $r(\tau')$, $\tau'<s$ when conditioned on $\eta(s)$ and $r(s)$. Hence, $\{x(t),r(t),\eta(t)\}$ is independent of the random variables $\{x(\tau'),r(\tau'),\eta(\tau')\}$, $\tau'<s$, when conditioned on $\{x(s),r(s),\eta(s)\}$, which establishes the Markov property of $\{x,r,\eta\}$.

In the analysis that follows, we will denote $f(x,\eta,u(x,r,t),t) \equiv f(x,r,\eta,t)$. We will now proceed to describe briefly the FDI process which monitors the random variations.

2.1 FDI Process

An FDI scheme is essentially an approach to a stochastic hypothesis testing problem. This hypothesis testing can be implemented using single sample tests, moving window tests or sequential tests. In single sample tests, the information used for the FDI tests is gathered, processed, and discarded at each time sample. In such cases, if the noise statistics on the information are white, then the FDI processing is memoryless, i.e. the future outcomes of the FDI tests are independent of the past and present outcomes if $\eta(t)$ and $r(t)$ remain fixed. Under these conditions, Markov models can be used to characterize the transition behavior of the state of the FDI process conditioned on the failure status of the components.

Any hypothesis testing algorithm has error probabilities associated with its decisions (Van Trees 1968). As a result, the FDI process state $r(t)$ (which is intended by design to follow the failure process state η) will deviate from $\eta(t)$ in the presence of false decisions and detection delays. Let us assume now that $\eta(t)$ is homogeneous. Since $r(t)$ is a Markov process when conditioned on $\eta(t)$ for single sample FDI tests acting on signals with additive white noise, the conditional probability $p_{ij}^{k}(\Delta t)$ that the $r(t)$ process will jump from state i to state j, $i,j\in S$, in an infinitesimal time interval of length Δt given that $\eta=k\in Z$ is,

$$p_{ij}^{k}(\Delta t) = q_{ij}^{k}\,\Delta t + o(\Delta t) \qquad (i\neq j) \tag{2.5}$$

Here, q_{ij}^{k} represents the transition rate from i to j for the Markov process $r(t)$ conditioned on $\eta=k\in Z$. Depending on the values of $i,j\in S$ and $k\in Z$, various interpretations, such as rate of false detection and isolation, rate of correct detection and isolation, false alarm recovery rate, etc., can be given to q_{ij}^{k}.

For the failure process $\eta(t)$, the transition probability from state i to state j, $i,j \in Z$, in the infinitesimal interval Δt is given by,

$$p_{ij}(\Delta t) = \alpha_{ij} \Delta t + o(\Delta t) \tag{2.6}$$

where α_{ij} are the transition rates of the homogeneous Markov process $\eta(t)$. In our case, the α_{ij} are related directly to the component failure rates.

3. DEFINITIONS

In this section, we will summarize some of the results on supermartingales that are relevant for our purposes. Also, we will present some definitions on stochastic stability and introduce the weak infinitesimal operator that is required in the analysis to follow. The material in this section is mostly drawn from Doob (1956), Kushner (1967) and Khasminskii (1980). In the discussion to follow, $\xi(t,\omega)=\xi(t)$ will denote a random process defined on the probability space $(\Omega, \mathcal{U}, P)$ which is $\mathcal{N}_t$-measurable for every $t \geq t_0$. Here, $\mathcal{N}_t \subset \mathcal{U}$ denotes a family of σ-algebras of events in Ω defined for every $t \geq t_0$. Further, $\mathcal{B}$ will denote the σ-algebra of Borel subsets on a closed interval $[t_0, t_1]=\mathcal{T}$.

To begin, we will formally define a Markov process and the *strong* Markov property. The stochastic process $\xi(t,\omega) \in \mathbb{R}^1$ will be called a Markov process if for $A \in \mathcal{B}$, $\tau \geq t_0$, and $t \geq 0$

$$P\left\{\xi(\tau+t,\omega) \in A \,|\, \mathcal{N}_\tau\right\} = P\left\{\xi(\tau+t,\omega) \in A \,|\, \xi(\tau,\omega)\right\} \tag{3.1}$$

with probability one. Here, $\mathcal{N}_\tau$ is the σ-algebra of events generated by all events of the form $\{\xi(u,\omega) \in A\}$, $u \leq \tau$ and $A \in \mathcal{B}$. If the above equality holds for any Markov time (Kushner 1967) τ, then $\xi(t,\omega)$ will be called a *strong* Markov process.

Let us again consider the stochastic process $\xi(t,\omega)=\xi(t)$ which is $\mathcal{N}_t$-measurable $\forall t \geq t_0$. Let $\xi(t)$ have finite expectation $E\{\xi(t)\} < \infty$ $\forall t \geq t_0$. Then the family $\{\xi(t), \mathcal{N}_t\}$ is called a *supermartingale* if for $s<t$, the following inequality holds with probability one:

$$E\{\xi(t)|\mathcal{N}_s\} \leq \xi(s) \tag{3.2}$$

If in (3.2), $\xi(t)>(\geq) 0\ \forall t\geq t_0$, then $\xi(t)$ is called a positive (nonnegative) supermartingale.

Theorem 3.1 (Doob 1956): If $\{\xi(t),\mathcal{N}_t\}$, $t\geq t_0$, is a positive supermartingale, then the limit $\xi_\infty = \lim_{t\to\infty} \xi(t)$ almost surely exists and is finite. Further, $E\{\xi_\infty\} = \lim_{t\to\infty} E\{\xi(t)\}$.

Theorem 3.2 (Doob 1956): If $\{\xi(t),\mathcal{N}_t\}$, $t\geq t_0$, is a non-negative supermartingale, then for any $\lambda>0$,

$$P\left\{\sup_{0\leq t\leq\infty} \xi(t)\geq\lambda\right\} \leq \frac{E\{\xi(0)\}}{\lambda} \tag{3.3}$$

The motivation for considering supermartingales here is that stochastic Lyapunov function candidates under certain conditions possess the supermartingale property. Hence, supermartingale theorems can be used to our advantage to study the stability of systems governed by stochastic differential equations. In the discussion to follow, $\mathcal{N}_t$ will denote the σ-algebra generated by the time history up to time t by any random process under consideration.

We will now present some definitions that are required in the analysis to follow.

Definition 3.1: The solution x=0 of system (2.1) is said to be almost surely stable in probability if for any $r_0\in S$, $\eta_0\in Z$, $\varepsilon>0$ and $\rho>0$, there exists a $\delta(\xi_0,\varepsilon,\rho)>0$ such that if $\|x_0\|<\delta(\xi_0,\varepsilon,\rho)$ we have,

$$P\left\{\sup_{0\leq t<\infty} \|x(t)\| \geq\varepsilon\right\} \leq \rho \tag{3.4}$$

Definition 3.2: The solution x=0 of system (2.1) is said to be almost surely asymptotically stable in probability if it is almost surely stable in probability and $x(t)\to 0$ with probability one as $t\to\infty$.

Definition 3.3: The solution x=0 of system (2.1) is said to be exponentially stable in the mean square if, for any $r_0 \in S$, $\eta_0 \in Z$ and some $\delta(r_0, \eta_0) > 0$ there exist two numbers a>0 and b>0 such that when $\|x_0\| \leq \delta(r_0, \eta_0)$, the following inequality holds for all solutions of (2.1) $\forall t \geq t_0$ with initial condition x_0:

$$E\left\{\|x(t)\|^2\right\} \leq b\|x_0\|^2 \exp\left[-a(t-t_0)\right] \tag{3.5}$$

Definition 3.4: A bounded function $f(\xi)$ is said to be in the domain of the weak infinitesimal operator $\mathcal{L}$ of the random process $\xi(t)$ if the limit

$$\lim_{\tau \to 0} \frac{E\{f(\xi(t+\tau))|\xi(t)\} - f(\xi(t))}{\tau} = \mathcal{L}f(\xi) = h(\xi) \tag{3.6}$$

exists pointwise in $\mathbb{R}$ and satisfies,

$$\lim_{\tau \to 0} E\{h(\xi(t+\tau))|\xi(t)\} = h(\xi(t)) \tag{3.7}$$

If we generalize Definition 3.4 to time varying functions $f(\xi, t)$, then we have

$$\mathcal{L}f(\xi, t) = \frac{\partial}{\partial t} f(\xi, t) + h(\xi, t) \tag{3.8}$$

In general, $\mathcal{L}f(\xi)$ is interpreted as the average time rate of change of the process $f(\xi)$ at time t given that $\xi(t)=\xi$.

Definition 3.5: Let $\xi(t)$ be a right continuous strong Markov process and τ a random time with $E\{\tau\}<\infty$. If the bounded function $f(\xi)$ is in the domain of $\mathcal{L}$ with $\mathcal{L}f(\xi)=h(\xi)$, then

$$E\{f(\xi(\tau))|\xi_0\} - f(\xi_0) = E\left\{\int_0^\tau h(\xi(s))ds \,\middle|\, \xi(0)\right\}$$

$$= E\{\int_0^{\tau} \mathcal{L}f(\xi(s))ds \,|\, \xi(0)\} \qquad (3.9a)$$

For time-varying functions, we have for every fixed $s<\tau$

$$E\{f(\xi(\tau),\tau)|\xi(s)\}-f(\xi(s),s) = E\{\int_s^{\tau}\left(\frac{\partial}{\partial t} f(\xi(s),s)+h(\xi(s),s)\right)ds\,|\,\xi(s)\}$$

$$= E\{\int_s^{\tau} \mathcal{L}f(\xi(s),s)ds \,|\, \xi(s)\} \qquad (3.9b)$$

Since $\xi(t)$ is a Markov process, there is no loss of generality when equation (3.9b) is conditioned on the σ-field $\mathcal{N}_s$ induced by the process $\xi(s)$. We shall assume this in our later analysis.

Equation (3.9) is referred to as Dynkin's formula. In our analysis, all Markov processes under consideration will be assumed to be strongly Markovian (a valid assumption for the case of Markov processes studied as models of physical processes) (Kushner 1967). We will now proceed to derive conditions for stochastic stability of the solution x=0 for (2.1).

4. STOCHASTIC STABILITY

In this section, we will derive conditions for almost sure asymptotic stability in probability and conditions for exponential stability in the mean square (ESMS) of the solution x=0 of the stochastic dynamical system (2.1). The tools for stability analysis will be stochastic Lyapunov functions and supermartingale theorems. In simple terms, a stochastic Lyapunov function is a suitable function of the state of the random differential equation that possesses the supermartingale property. From the existence of such functions, the asymptotic and finite time properties of the random trajectories of the stochastic differential equations can be inferred. We will now define the notion of a stochastic Lyapunov function candidate (Kats and Krasovskii 1960, Kushner 1967) and derive conditions for it to possess the supermartingale property.

Let us consider the function $V(x,r,\eta,t)$ of the joint Markov process $\{x,r,\eta\}$. For fixed $m<\infty$, let the following conditions hold:

(a) The function $V(x,r,\eta,t)$ is positive definite and continuous in x and t

in the open set $O_m=\{x(t): V(x,r,\eta,t)<m\}$ $\forall r\in S$, $\forall\eta\in Z$ and $\forall t\geq t_0$, and $V(x,r,\eta,t)=0$ only if $x=0$. (The function $V(x,r,\eta,t)$ is said to be positive definite if $V(x,r,\eta,t)\geq W(x)$ $\forall r\in S$, $\forall\eta\in Z$ and $\forall t\geq t_0$, where $W(x)$ is positive definite in the sense of Lyapunov)

(b) The joint Markov process $\{x,r,\eta\}$ is defined until at least some $\tau_m=\inf\{t: x(t)\notin O_m\}$ (or, $\forall t<\infty$ if $x(t)\in O_m$ for $t<\infty$). If $x(t)\in O_m$ $\forall t<\infty$, then $\tau_m=\infty$.

(c) The function $V(x,r,\eta,t)$ is in the domain of $\mathcal{L}$ where $\mathcal{L}$ is the weak infinitesimal operator of the joint Markov process $\{x(\tau_t), r(\tau_t), \eta(\tau_t)\}$, where $\tau_t=\min(t,\tau_m)$.

A function $V(x,r,\eta,t)$ that satisfies the above conditions will be said to qualify as a stochastic Lyapunov function candidate for (2.1). We will now prove the following lemma that establishes the supermartingale property of the function $V(x(\tau_t), r(\tau_t), \eta(\tau_t), \tau_t)$.

Lemma 4.1: Let the random function $V(x,r,\eta,t)$ satisfy assumptions (a)-(c) above and let $x_0\in O_m$. Further, let $\mathcal{L}V(x,r,\eta,t)\leq 0$ in the open set O_m. Then $V(x(\tau_t), r(\tau_t), \eta(\tau_t), \tau_t)$ is a positive supermartingale.

Proof:

Applying Dynkin's formula we have,

$$E\{V(x(\tau_t), r(\tau_t), \eta(\tau_t), \tau_t)\,|\,\mathcal{N}_s\}-V(x(s), r(s), \eta(s), s)$$

$$= E\{\int_s^{\tau_t} \mathcal{L}V(x(\tau), r(\tau), \eta(\tau), \tau)d\tau\,|\,\mathcal{N}_s\} \leq 0 \qquad (t_0\leq s<\tau_t) \qquad (4.1)$$

In (4.1), $\mathcal{N}_s$ is the σ-algebra generated by the process $\{x,r,\eta\}$ up to time s. From (4.1), it follows that

$$E\{V(x(\tau_t), r(\tau_t), \eta(\tau_t), \tau_t)\,|\,\mathcal{N}_s\}\leq V(x(s), r(s), \eta(s), s)<\infty \qquad (s<\tau_t) \qquad (4.2)$$

From the above equation and the positive definiteness of $V(x,r,\eta,t)$, we see that $V(x(\tau_t), r(\tau_t), \eta(\tau_t), \tau_t)$ is a positive supermartingale of the stopped process $\{x(\tau_t), r(\tau_t), \eta(\tau_t)\}$.

The conditions for stochastic stability of the solution x=0 of the system (2.1) will now be derived using the above result.

4.1 Conditions for Stability in Probability

The following theorem gives sufficient conditions for almost sure stability in probability for the solution x=0 of the system (2.1).

Theorem 4.1: Let us assume that conditions (a)-(c) given above hold. Further, let $\mathcal{L}V(x,r,\eta,t)\leq 0$ in the open set O_m for $r\in S$ and $\eta\in Z$ for (2.1). Then the solution x=0 of (2.1) is almost surely stable in probability.

Proof:

From Lemma 4.1, it follows that for $x_0\in O_m$, $V(x(\tau_t),r(\tau_t),\eta(\tau_t),\tau_t)$ is a positive supermartingale. Here, $\tau_t=\min(t,\tau_m)$, where τ_m is the first exit time of x(t) from O_m. Consider the sequence of Markov times $\{\tau_m\}$ as $m\to\infty$. Then, it is easy to see that τ_m defines a non-decreasing sequence of Markov times such that $\tau_m\to\infty$ with probability one as $m\to\infty$. (The proof follows immediately from Theorem 3.2).

Further, from Theorem 3.1 the following limit almost surely exists and is finite:

$$\lim_{\tau_t\to\infty} V(x(\tau_t),r(\tau_t),\eta(\tau_t),\tau_t) = V_\infty < \infty \qquad (4.3)$$

It follows from (4.3) that $V(x,r,\eta,t)$ is bounded $\forall t\geq t_0$. From this and for $x_0\in O_m$, it can be shown that $V(x,r,\eta,t)$ is a positive supermartingale. Hence, from Theorem 3.2, we have for any $\varepsilon'>0$,

$$P\left\{\sup_{0\leq t<\infty} V(x,r,\eta,t)\geq\varepsilon'\right\} \leq \frac{V(x_0,r_0,\eta_0,t_0)}{\varepsilon'} \qquad (4.4)$$

Under the assumptions (a)-(c) on $V(x,r,\eta,t)$, it follows that $V(x,r,\eta,t)\to 0$ as $x\to 0$. Hence, for a suitable choice of $x_0\in O_m$, we have for any $r_0\in S$, $\eta_0\in Z$, $\varepsilon'>0$ and $\rho>0$,

$$P\left\{\sup_{0\le t<\infty} V(x,r,\eta,t)\ge\varepsilon'\right\} \le \rho \qquad (4.5)$$

Further, from the positive definiteness of $V(x,r,\eta,t)$, it follows that there exists a function $W(x)$ which is positive definite in the sense of Lyapunov such that,

$$V(x,r,\eta,t) \ge W(x) \ge \alpha\|x(t)\| \qquad (\alpha>0) \qquad (4.6)$$

From the above equation, we can see easily that for $\varepsilon=(\varepsilon'/\alpha)>0$,

$$P\left\{\sup_{0\le t<\infty} \|x(t)\|\ge\varepsilon\right\} \le \rho \qquad (4.7)$$

Hence, the proof is complete.

For the class of functions $V(x,r,\eta,t)=V$ of the joint Markov process $\{x,r,\eta\}$ satisfying the assumptions (a)-(c) above, the weak infinitesimal operator $\mathcal{L}$ of the process $\{x,r,\eta\}$ for the system (2.1) at the point $\{x,r=i,\eta=k,t\}$ is given by,

$$\mathcal{L}V = \frac{\partial V}{\partial t} + \langle f(x,i,k,t), \frac{\partial V}{\partial x}\rangle + \sum_{\substack{j\in S\\ j\neq i}} q_{ij}^{k}\,[V(x,j,k,t)-V(x,i,k,t)]$$

$$+ \sum_{\substack{j\in Z\\ j\neq k}} \alpha_{kj}\,[V(x,i,j,t)-V(x,i,k,t)] \qquad (4.8)$$

Recall that in the above equation, α_{kj}, $k,j\in Z$ are the transition rates of the $\eta(t)$ process from state $\eta=k$ to state $\eta=j$ and q_{ij}^{k}, $k\in Z$ and $j\in S$, are the conditional transition rates of the FDI process state from $r=i$ to $r=j$ (conditioned on $\eta=k$), which were defined in chapter 2. The first term in (4.8) occurs due to incremental changes in the function $V(x,r,\eta,t)$ when x, r and η are constant. The second term in (4.8) is the increment in the Lyapunov function due to changes in x in an infinitesimal interval when r and η are fixed. The third term in (4.8) is the change in the stochastic Lyapunov function in an infinitesimal interval when $r(t)$ transitions from state i to j, $(i,j\in S)$ given that $\eta=k\in Z$. The last term in (4.8) is due to the

incremental changes in the stochastic Lyapunov function when $\eta(t)$ transitions from the state k to j, $(k, j \in Z)$.

The following theorem gives sufficient conditions for almost sure asymptotic stability in probability.

Theorem 4.2: Assume conditions (a)-(c) given above hold. Further, let $\mathcal{L}V(x,r,\eta,t) = -K(x,r,\eta,t) < 0$ in the open set O_m for (2.1) when $r \in S$ and $\eta \in Z$, where $K(x,r,\eta,t) > 0$ and continuous in x $\forall t \geq t_0$, and $K(x,r,\eta,t) = 0$ only if x=0. Then the solution x=0 of (2.1) is almost surely asymptotically stable in probability.

Proof:

Under the conditions stated above, the solution x=0 of (2.1) is almost surely stable in probability (follows from Theorem 4.1). Also, we know that $V(x,r,\eta,t)$ is a positive supermartingale. From the inequality (4.2) and the positive definiteness of $V(x,r,\eta,t)$ (and hence non-negativity of the conditional expectation), it follows that the left hand side of (4.1) is bounded $\forall \tau_t \geq t_0$. Now, let us denote the total time spent in the set $\{x: K(x,r,\eta,t) \geq \varepsilon > 0\} \cap O_m$ during the interval $[t, \tau_m)$ by $T(t,\varepsilon)$. Then, for $\tau_m = \infty$ it follows from (4.1) that

$$\infty > V(x_0, r_0, \eta_0, t_0) \geq E\{\int_t^\infty K(x(s), r(s), \eta(s), s)ds \,|\, \mathcal{N}_s\} \geq \varepsilon E\{T(t,\varepsilon)\} \qquad (4.9)$$

The above equation implies that $T(t,\varepsilon) < \infty$ with probability one, and hence, as $t \to \infty$ in (4.9), $T(t,\varepsilon) \to 0$ with probability one. In other words, $K(x,r,\eta,t) \to 0$ as $t \to \infty$ with probability one. Since $K(x,r,\eta,t)$ is continuous in x $\forall t \geq t_0$, this implies that $x(t) \to 0$ as $t \to \infty$ with probability one. This completes the proof.

4.2 Conditions for Exponential Stability

In this section, we will derive necessary and sufficient conditions for exponential stability in the mean square (in the sense of Definition 3.3) for the general dynamic system given by (2.1). We point out that using these conditions, it is difficult to verify the exponential stability in the mean square of a general stochastic dynamic system of the form (2.1). However, if we consider the linear plant model (2.2), then it is easy to verify whether

the system is stable in the sense of Definition 3.3 or not. We will examine this particular case in section 5.

The following theorem gives a sufficient condition for exponential stability in the mean square sense for the system (2.1).

Theorem 4.3: The solution x=0 of the system (2.1) is exponentially stable in the mean square for $t \geq t_0$ if there exists a function $V(x,r,\eta,t)$ satisfying the conditions (a)-(c) in section 4 such that,

$$k_1\|x(t)\|^2 \leq V(x,r,\eta,t) \leq k_2\|x(t)\|^2 \tag{4.10}$$

and $$\mathcal{L}V(x,r,\eta,t) \leq -k_3\|x(t)\|^2 \tag{4.11}$$

for some positive constants k_1, k_2 and k_3.

Proof:

It can be shown that the condition (4.11) is sufficient to ensure $V\{x(\tau_t), r(\tau_t), \eta(\tau_t), \tau_t\}$ is a positive supermartingale. This implies that the limit (4.3) exists and hence, $V(x,r,\eta,t)$ has finite expectation $\forall t \geq t_0$. Applying Dynkin's formula to the bounded function $V(x,r,\eta,t)$ of the Markov process $\{x,r,\eta\}$, we have for any $t<\infty$

$$E\{V(x,r,\eta,t)\,|\,x_0,r_0,\eta_0\} - V(x_0,r_0,\eta_0,t_0)$$

$$= E\{\int_{t_0}^{t} \mathcal{L}V(x,r,\eta,t)ds\,|\,x_0,r_0,\eta_0\} \tag{4.12}$$

Taking expectations on both sides of equation (4.12) and differentiating with respect to t, we obtain

$$\frac{d}{dt}E\{V(x,r,\eta,t)\} = E\{\mathcal{L}V(x,r,\eta,t)\} \tag{4.13}$$

Taking the expectations of the inequalities (4.10) and (4.11) and substituting on the right hand side of (4.13), we have

$$\frac{d}{dt}E\{V(x,r,\eta,t)\} \leq -\frac{k_3}{k_2} E\{V(x,r,\eta,t)\} \tag{4.14}$$

Integrating both sides of (4.14) with respect to t, we obtain the inequality

$$E\{V(x,r,\eta,t)\} \leq V(x_0,r_0,\eta_0,0)\ \exp\left(-\frac{k_3}{k_2}\ t\right) \tag{4.15}$$

Again, taking the expectation of (4.10) and substituting for $E\{V(x,r,\eta,t)\}$, we get the relation

$$E\{\|x(t)\|^2\} \leq \frac{k_2}{k_1}\ \|x_0\|^2\ \exp\left(-\frac{k_3}{k_2}\ t\right), \qquad t\geq t_0 \tag{4.16}$$

The proof is complete.

A necessary condition for exponential stability in the mean square for (2.1) is given by the following theorem:

Theorem 4.4: If the solution x=0 of the system (2.1) is exponentially stable in the mean square, then there exists a function $V(x,r,\eta,t)$ $\forall r\in S$ and $\forall\eta\in Z$ that is continuous $\forall t\geq t_0$ and satisfies conditions (4.10) and (4.11) for some positive constants k_1, k_2 and k_3.

Proof:

Let us define the function $V(x,r.\eta,t)$ as

$$V(x,r,\eta,t) = \int_t^{t+T} E\{\|x(\tau)\|^2\}d\tau \tag{4.17}$$

We shall show that (4.17) satisfies all the conditions of the theorem for a suitable choice of T. If the solution x=0 of (2.1) is exponentially stable in the mean square, it follows from Definition 3.3 that for some $\alpha>0$ and $\beta>0$,

$$E\{\|x(\tau)\|^2\} \leq \alpha\|x(t)\|^2\ \exp\left(-\beta(\tau-t)\right), \qquad \tau\geq t \tag{4.18}$$

Substituting for $E\{\|x(\tau)\|^2\}$ from (4.18) into (4.17) we obtain

$$V(x,r,\eta,t) \le \alpha\|x(t)\|^2 \int_t^{t+T} \exp\Big(-\beta(\tau-t)\Big)d\tau \tag{4.19}$$

For a suitable choice of T>0, it follows that

$$V(x,r,\eta,t) \le k_2\|x(t)\|^2, \qquad (k_2>0) \tag{4.20}$$

Further, every realization of a solution to (2.1) satisfies the condition

$$E\Big\{\|x(t)\|^2\Big\} \ge \|x_0\|^2 \exp(-2nLt) \tag{4.21}$$

where L satisfies the Lipschitz condition defined in (2.3) and n is the dimension of x. From this we obtain

$$\begin{aligned} V(x,r,\eta,t) &= \int_t^{t+T} E\{\|x(\tau)\|^2\}d\tau \\ &\ge \int_t^{t+T} \|x(t)\|^2 \exp(-2nL(\tau-t))d\tau \\ &= \|x(t)\|^2 \int_t^{t+T} \exp(-2nL(\tau-t))d\tau \end{aligned} \tag{4.22}$$

From (4.22), the following inequality follows for any k_1 such that $0<k_1\le\frac{1-\exp(-2nLT)}{2nL}$:

$$V(x,r,\eta,t) \ge k_1\|x(t)\|^2, \tag{4.23}$$

From (4.19) and (4.23), we see that the condition (4.10) is satisfied.

To show that $V(x,r,\eta,t)$ is in the domain of $\mathcal{L}$ (and hence continuous) and the relation (4.11) is satisfied, we proceed as follows. By the definition of $\mathcal{L}$ we have,

$$\mathcal{L}V = \lim_{\delta \to 0} \frac{E\{V(x(t+\delta), r(t+\delta), \eta(t+\delta), t+\delta) | \mathcal{F}\} - V(x, r, \eta, t)}{\delta} \qquad (4.24)$$

where $\mathcal{F}=(x(t), r(t), \eta(t))$. From (4.17) and (4.24) we have,

$$\mathcal{L}V = \lim_{\delta \to 0} \frac{1}{\delta} \left[E\{ \int_{t+\delta}^{t+T+\delta} E\{\|x(\tau)\|^2\} d\tau | \mathcal{F}\} - \int_{t}^{t+T} E\{\|x(\tau)\|^2\} d\tau \right] \qquad (4.25)$$

From (4.25) and the inequality (4.18), we can show that

$$\mathcal{L}V \leq \lim_{\delta \to 0} \frac{1}{\delta} \alpha \left[\|x(t)\|^2 \int_{t+\delta}^{t+T+\delta} \exp\left(- \beta(\tau - t) \right) d\tau \right.$$

$$\left. - \|x(t)\|^2 \int_{t}^{t+T} \exp\left(- \beta(\tau - t) \right) d\tau \right] \qquad (4.26)$$

Evaluating the integrals in (4.26) and after further simplification, we obtain the following inequality:

$$\mathcal{L}V \leq \alpha \|x(t)\|^2 \frac{1}{\beta} \lim_{\delta \to 0} \left[e^{-\beta T} \frac{(1 - e^{-\beta\delta})}{\delta} - \frac{(1 - e^{-\beta\delta})}{\delta} \right] \qquad (4.27)$$

Taking limits in (4.27) it can be shown after some simplification that

$$\mathcal{L}V(x, r, \eta, t) \leq \alpha \left(e^{-\beta T} - 1 \right) \|x(t)\|^2 \qquad (\alpha, \beta, T > 0)$$

$$\leq -k_3 \|x(t)\|^2 \qquad (4.28)$$

for any $k_3 \geq \alpha(1 - \exp(-\beta T)) > 0$. Hence, the proof is complete.

Before concluding this section, we mention that for linear dynamical systems of the form (2.2) the following lemma is true:

Lemma 4.2: If the solution x=0 of (2.2) is exponentially stable in the mean

square, then for any given quadratic positive definite function $W(x,r,\eta,t)$ in the variables x which is bounded and continuous $\forall t \geq t_0$, $\forall r \in S$ and $\forall \eta \in Z$, there exists a quadratic positive definite function $V(x,r,\eta,t)$ in x that satisfies conditions (4.10) and (4.11) and is such that $\mathcal{L}V(x,r,\eta,t) = -W(x,r,\eta,t)$.

The proof for this lemma follows by selecting the function $V(x,r,\eta,t)$ as follows:

$$V(x,r,\eta,t) = \int_t^{t+T} E\{W(x,r,\eta,\tau)\}d\tau \qquad (4.29)$$

It is easy to verify using arguments similar to those used for proving Theorem 4.4 that for this choice of $V(x,r,\eta,t)$, the conditions in Lemma 4.2 hold for the linear plant model (2.2).

We will now apply the results derived in this section to obtain conditions that will enable us to verify the exponential stability in the mean square of the linear plant model (2.2) under any linear time-invariant state feedback control law dependent on the FDI process state.

5. NECESSARY AND SUFFICIENT CONDITIONS FOR EXPONENTIAL STABILITY

As pointed out earlier, the results in section 4.2 are difficult to apply to check the exponential stability in the mean square of a general dynamical system described by (2.1). In this section, conditions that allow us to verify whether or not the linear plant model (2.2) under the control law $u(x,r)=K(r)x(t)$ has exponential stability in the mean square will be derived. We will denote this control law by $u_i=-K_i x$ when $r=i \in S$. For the time-invariant case, we will assume without loss of generality that $t_0=-\infty$. The results in this section will be useful in synthesizing a fault tolerant feedback control law that ensures the stochastic stability of the linear plant model (2.2). This will be discussed in the companion paper (Srichander and Walker, 1990).

Theorem 5.1: A necessary and sufficient condition for exponential stability in the mean square of the linear plant model (2.2) under the control law $u_i=-K_i x$, $i \in S$, is that there exist steady state solutions $P_{ik}>0$, $i \in S$, $k \in Z$ as $t \to -\infty$ to the following coupled linear matrix differential equations:

$$\dot{P}_{ik}(t) + \tilde{A}_{ik}^T P_{ik}(t) + P_{ik}(t)\tilde{A}_{ik} + \sum_{\substack{j\in S \\ j\neq i}} q_{ij}^k P_{jk}(t)$$

$$+ \sum_{\substack{j\in Z \\ j\neq k}} \alpha_{kj} P_{ij}(t) + Q_{ik} = 0, \quad i\in S, \quad k\in Z, \quad t\in(-\infty, 0] \qquad (5.1)$$

with boundary conditions,

$$P_{ik}(0) = 0, \quad \forall i\in S, \quad \forall k\in Z \qquad (5.2)$$

where $Q_{ik}>0$, $\forall i\in S$, $\forall k\in Z$, and

$$\tilde{A}_{ik} = A - B_i K_i - 0.5 \sum_{\substack{j\in S \\ j\neq i}} q_{ij}^k - 0.5 \sum_{\substack{j\in Z \\ j\neq k}} \alpha_{jk}, \quad i\in S, \quad k\in Z \qquad (5.3)$$

Proof of necessity:

Assume that (2.2) is exponentially stable in the mean square under the control law $u_i=-K_i x$, $\forall i\in S$. Let $W(x,r,\eta,t)=x^T Q(r,\eta)x$, $r\in S$, $\eta\in Z$ denote a quadratic positive definite function. Then it follows from Lemma 4.2 that there exists a quadratic positive definite function $V(x,r,\eta,t)$ $\forall r\in S$ and $\forall\eta\in Z$ that satisfies the condition (4.10) and is in the domain of the weak infinitesimal operator $\mathcal{L}$ such that $\mathcal{L}V(x,r,\eta,t)=-W(x,r,\eta,t)$. Let us denote the quadratic function that satisfies these conditions by $V(x,r,\eta,t)=x^T P(r,\eta,t)x$. We shall denote in the sequel $Q(r,\eta)=Q_{ik}$ and $P(r,\eta,t)=P_{ik}(t)$ when $r=i\in S$ and $\eta=k\in Z$.

Evaluating the function $\mathcal{L}V(x,r,\eta,t)$ for (2.2) under the control law $u_i=-K_i x$ when the quantities $r=i\in S$ and $\eta=k\in Z$ have occurred at some time $t\in(-\infty,0]$, we can show after some simplification that

$$\mathcal{L}V = x^T\Big[\dot{P}_{ik}(t) + \tilde{A}_{ik}^T P_{ik}(t) + P_{ik}(t)\tilde{A}_{ik} + \sum_{\substack{j\in S \\ j\neq i}} q_{ij}^k P_{jk}(t)$$

$$+ \sum_{\substack{j\in Z \\ j\neq k}} \alpha_{kj} P_{ij}(t)\Big]x, \quad i\in S, \quad k\in Z \tag{5.4}$$

where $\tilde{A}_{ik}^T$ is given by (5.3). Further, since $\mathcal{L}V(x,r,\eta,t) = -W(x,r,\eta,t)$, we have the identity

$$x^T\Big[\dot{P}_{ik}(t) + \tilde{A}_{ik}^T P_{ik}(t) + P_{ik}(t)\tilde{A}_{ik} + \sum_{\substack{j\in S \\ j\neq i}} q_{ij}^k P_{jk}(t)$$

$$+ \sum_{\substack{j\in Z \\ j\neq k}} \alpha_{kj} P_{ij}(t) + Q_{ik}\Big]x = 0, \quad i\in S, \quad k\in Z \tag{5.5}$$

We note in particular that the quantity inside the brackets of (5.5) is identical to the coupled matrix differential equations given by (5.1).

Let us examine the solutions to (5.1) under the boundary conditions (5.2). We shall denote by $\Phi_{ik}(t,\tau)$ the fundamental matrix associated with $\tilde{A}_{ik}$, i.e.,

$$\Phi_{ik}(t,\tau) = \exp(\tilde{A}_{ik}(t-\tau)), \quad i\in S, \quad k\in Z, \quad -\infty<\tau\le t\le 0 \tag{5.6}$$

Then, it is easy to check that under (5.1) and (5.2) the solutions $P_{ik}(t)$, $i\in S$, $k\in Z$ are given by,

$$P_{ik}(t) = \int_t^0 \Phi_{ik}^T(t,\tau)\Big[\sum_{\substack{j\in S \\ j\neq i}} q_{ij}^k P_{jk}(\tau) + \sum_{\substack{j\in Z \\ j\neq k}} \alpha_{kj} P_{ij}(\tau)$$

$$+ Q_{ik}\Big]\Phi_{ik}(t,\tau)d\tau, \quad i\in S, \quad k\in Z, \quad t\in(-\infty,0) \tag{5.7}$$

The coupled integral equations given by (5.7) have unique solutions $\{P_{ik}(t),\ i\in S,\ k\in Z\}$ that are continuous on $t\in(-\infty,0)$. Further, since $\Phi_{ik}(t,\tau)$, $\forall i\in S$, $\forall k\in Z$ are non-singular for $t,\tau\in(-\infty,0]$ and $Q_{ik}>0$, $\forall i\in S$, $\forall k\in Z$, it follows immediately from (5.7) that $P_{ik}(t)>0$, $\forall i\in S$, $\forall k\in Z$ for $t\in(-\infty,0)$. Also, from

the positive definiteness of $P_{ik}(t)$, $\forall i\in S$, $\forall k\in Z$ and the non-negativity of the transition rates of $r(t)$ and $\eta(t)$, it follows from (5.7) that the solutions $P_{ik}(t)$, $\forall i\in S$, $\forall k\in Z$ are monotonically increasing on $(-\infty,0]$ as t decreases. Since, from Lemma 4.2, we know that $V(x,r,\eta,t)$ satisfies the condition (4.10), the solutions $\{P_{ik}(t),\ i\in S,\ k\in Z\}$ are bounded on $t\in(-\infty,0]$. In other words, as t decreases, the $P_{ik}(t)$, $\forall i\in S$, $\forall k\in Z$, define a set of monotone increasing sequences of positive operators on $t\in(-\infty,0]$ that are bounded from below. We now state a lemma for positive operators in Hilbert space to prove the convergence of the sequence $\{P_i(t), i\in S\}$.

Lemma 5.1 (Akhiezer and Glazman 1981): Every monotonically increasing sequence of bounded positive operators in Hilbert space converges strongly.

From the above lemma, it follows immediately that the solutions converge to steady state solutions $\{P_{ik}>0,\ i\in S,\ k\in Z\}$ as $t\to-\infty$. Hence, the necessary condition is proven.

Proof of sufficiency:

Let us assume that there exist steady state solutions $\{P_{ik}>0,\ i\in S,\ k\in Z\}$ as $t\to-\infty$ to the coupled differential equations (5.1) under the boundary conditions (5.2). Then, it is easy to see that the function $V(x,r,\eta,t)=x^TP(r,\eta)x$ satisfies the conditions (a)-(c) in section 4 and also the condition (4.10). Evaluating $\mathcal{L}V(x,r,\eta,t)$ for the linear plant model (2.2) under the control law $u_i=-K_ix$, $i\in S$ when the quantities $r=i\in S$ and $\eta=k\in Z$ have occurred at some time $t\in(-\infty,0]$, we have,

$$\mathcal{L}V = x^T\left[\tilde{A}_{ik}^T P_{ik} + P_{ik}\tilde{A}_{ik} + \sum_{\substack{j\in S\\ j\neq i}} q_{ij}^k P_{jk} + \sum_{\substack{j\in Z\\ j\neq k}} \alpha_{kj} P_{ij}\right]x,\quad i\in S,\ k\in Z \qquad (5.8)$$

where $\tilde{A}_{ik}$ is given by (5.3). Since by hypothesis $\{P_{ik},\ i\in S,\ k\in Z\}$ satisfies (5.1), we have $\mathcal{L}V(x,r,\eta,t)=-W(x,r,\eta,t)$. Further, since $W(x,r,\eta,t)$ is positive definite $\forall r\in S$ and $\forall\eta\in Z$, it follows from Theorem 5.1 that (2.2) under the control law $u_i=-K_i$, $i\in S$ is exponentially stable in the mean square $\forall t\geq t_0$. Hence, the proof is complete.

Remarks on Theorem 5.1:

The stochastic stability analysis presented here takes into account the decision errors and delays associated with the FDI decision making process. Most of the results on fault tolerant control systems available in the literature so far (see Ji and Chizeck 1990, Sworder 1969, Wonham 1971), do not account for these decision errors and delays, and hence, do not ensure stability of the solution x=0 of the linear plant model (2.2) that describes the behavior of a true active fault tolerant control system. The stability analysis for these systems investigated by Mariton accounts only for the delayed decisions and false alarms of the FDI schemes. The stability analysis presented by Mariton (1989) assumes that correct failure isolation is done following a failure and that the state spaces of the FDI and failure processes are identical. These assumptions are questionable in real systems where the FDI scheme might involve a failure detection phase and a failure isolation phase (Walker 1980) and incorrect failure isolation can result following the detection of the presence of a failure. Thus, the analysis of Mariton (198910 is also inadequate to ensure the stability of active fault tolerant control systems. Hence, the results derived in this section are a significant contribution towards the stability analysis of active fault tolerant control systems that reconfigure the control gains using information from the FDI scheme.

We shall now show that the results on the JLQR problem investigated by Wonham (1971) can be derived as a special case of the results in this section. For the JLQR problem, it is assumed that the transitions of the failure process $\eta(t)$ are detected instantaneously, which implies $r(t)=\eta(t)$ $\forall t \geq t_0$. Hence, we need to consider only the cases where $r=\eta=i \in S$, and analyze the stochastic stability of the linear plant model under any control law of the form $u_i=-K_i x$, $i \in S$. It is obvious from the assumption of instantaneous detection that when $j \neq i \in S$, we have $q_{ij}^i=0$. Hence, when $r=\eta=i \in S$, it follows that

$$\tilde{A}_{ii} = A - B_i K_i - 0.5I \sum_{\substack{j \in S \\ j \neq i}} \alpha_{ij} , \quad i \in S \tag{5.9}$$

When the $\tilde{A}_{ik}$ in (5.1) are replaced by the $\tilde{A}_{ii}$, $i \in S$, defined above, then the results for the JLQR problem derived by Wonham (1971) are obtained as special cases of the sufficient conditions for stability given by Theorem 5.1.

We mention finally that if the linear plant model (2.2) is exponentially stable in the mean square, then it is almost surely asymptotically stable in probability. The proof follows immediately from Theorems 4.2 and 4.4. Thus, if the conditions in Theorem 5.1 are satisfied, then the linear plant model (2.2) under the control law $u_i=-K_i x$, $i\epsilon S$ is almost surely asymptotically stable in probability. In other words, the existence of steady state solutions $\{P_{ik}>0,\ i\epsilon S,\ k\epsilon Z\}$ implies that the plant model is almost surely asymptotically stable in probability.

6. CONCLUSIONS

The stochastic stability of fault tolerant control systems incorporating a real time reconfiguration strategy based on FDI decisions has been addressed in this paper. In particular, *necessary and sufficient* conditions for exponential stability in the mean square of linear fault tolerant control systems were derived. It is shown that these conditions are also sufficient for almost sure asymptotic stability in probability. The results in this paper are also shown to be an extension to the earlier results on JLQR problems, where instantaneous detection of mode transitions of the failure process is assumed. Since such an assumption is invalid when a realistic FDI scheme subject to errors and delays is used to detect these changes, the results in this paper are significant contributions toward the stability analysis of actively reconfigurable fault tolerant control systems. As already pointed out, the earlier results on reconfigurable control systems have the drawback of addressing only the deterministic stability of the closed loop system after the FDI scheme has correctly identified the failures. Such an analysis does not guarantee the stochastic stability of the solution x=0 for the system under incorrect failure isolation for all FDI transition rates. This will be illustrated by means of a numerical example for the linear plant model (2.2) in the companion paper (Srichander and Walker, 1990).

ACKNOWLEDGMENT

This work was supported by the Air Force Office of Scientific Research under grant AFOSR-89-0486 DEF.

REFERENCES

AKHIEZER, N. I., and GLAZMAN, I. M., 1981, *Theory of Linear Operators in Hilbert Space, Vol II*, Pitman Publishing, London.

BERTRAM, J. E., and SARACHICK, P. E., 1959, Stability of Circuits with Randomly Time-Varying Parameters, *Trans. Inst. Radio Engr.*, 5, 260-270.

BUCY, R. S., 1965, Stability and Positive Supermartingales, *J. of Diffl. Eqns.*, **1**, 151-155.

CAGLAYAN, A. K., RAHNAMAI, K., MOERDER, D. D., and HALYO, N., 1987, A Hierarchical Reconfiguration Strategy for Aircraft Subjected to Actuator Failure/Surface Damage, Air Force Wright Aeronautics Lab., Wright Patterson AFB, Ohio, AFWAL-TR-87-3034.

DOOB, J. L., 1956, *Stochastic Process*, Wiley, New York.

HOWELL, W., BUNDICK, T., HUESCHEN, R., and OSTROFF, A., 1983, Restructurable Controls for Aircraft, *AIAA Guidance and Control Conference*, Gatlinburg, Tennessee, AIAA-83-2255.

JI, Y., and CHIZECK, H. J., 1990, Controllability, Stabilizability, and Continuous-Time Markovian Jump Linear Quadratic Control, *I.E.E.E. Trans. Autom. Control*, 35, 777-788.

KATS, I. IA., and KRASOVSKII, N. N., 1960, On Stability of Systems with Random Parameters, *J. of Appl. Math. and Mech.*, **24**, 1225-1246.

KHASMINSKII, R. Z., 1962, On the Stability of the Trajectory of Markov Processes, *J. Appl. Math. Mech.*, **26**, 1554-1565.

KHASMINSKII, R. Z., 1967, Necessary and Sufficient Conditions for Asymptotic Stability of Linear Stochastic Systems, *Theory of Prob. and Appl.*, **12**, 144-147.

KHASMINSKII, R. Z., 1980, *Stochastic Stability of Differential Equations*, Sijthoff and Noordhoff, Netherlands.

KOZIN, F., 1969, A Survey of Stability of Stochastic Systems, *Automatica*, **5**, 95-112.

KOZIN, F., 1972, Stability of the Linear Stochastic System, *Lecture Notes in Mathematics*, **294**, Springer Verlag, Berlin, 186-229.

KUSHNER, H. J., 1967, *Stochastic Stability and Control*, Academic Press, New York.

KUSHNER, H. J., 1971, *Introduction to Stochastic Control*, Holt, Rinehart and Winston, Inc., New York.

KUSHNER, H. J., 1972, Stochastic Stability, *Lecture Notes in Mathematics*,

294, Springer Verlag, Berlin, 97-124.

LOOZE, D., KROLEWSKI, S., WEISS, J., BARRETT, N., and ETERNO, J., 1984, Automatic Control Design Procedures for Restructurable Aircraft Control, NASA Contractor Report CR-172489.

LOOZE, D. P., WEISS, J. L., ETERNO, J. S., and BARRETT, N. M., 1985, An Automatic Redesign Approach for Restructurable Control Systems, *I.E.E.E. Control Systems Mag.*, 5, 16-22.

MARITON, M., 1989, Detection Delays, False Alarm Rates and the Reconfiguration of Control Systems, *Int. J. Control*, **49**, 981-992.

MOERDER, D. D., HALYO, N., BROUSSARD, J. R., and CAGLAYAN, A. K., 1989, Application of Precomputed Control Laws in a Reconfigurable Aircraft Flight Control System, *J. of Guidance, Control and Dynamics*, **12**, 325-333.

NEVELSON, M. B., 1966, Stability in the Large of a Trajectory of the Markov Processes of Diffusion-Type, *J. of Diffl. Eqns.*, 2, 544-548.

PATTON, R. J., FRANK, P. M., and CLARK, R. N., (*eds.*), 1989, *Fault Diagnosis in Dynamic Systems: Theory and Applications*, Prentice Hall, London.

PETKOVSKI, Dj. B., 1987, Multivariable Control Systems Design: A Case Study of Robust Control of Nuclear Power Plants, in *Fault Detection and Reliability*, Vol 9, Pergamon Press, New York, 239-246.

POTTER, J. E., and SUMAN, M. C., 1986, Extension of Midvalue Selection Technique for Redundancy Management of Inertial Sensors, *J. of Guidance, Control and Dynamics*, 9, 37-44.

SRICHANDER, R., 1990, Fault Tolerant Control of Continuous Time Systems, Ph. D. dissertation, Dept. of Aerospace Engg. and Engg. Mechanics, University of Cincinnati, Cincinnati.

SRICHANDER, R., and WALKER, B. K., 1990, The Synthesis and Stability of a Feedback Control Law for Continuous Time Fault Tolerant Control Systems, submitted to *Int. J. Control*.

SWORDER, D. D., 1969, Feedback Control of a Class of Linear Systems with Jump Parameters, *I.E.E.E. Trans. Autom. Control*, **14**, 9-14.

VAN TREES, H. L., 1968, *Detection, Estimation and Modulation Theory*, Wiley, New york.

VIDYASAGAR, M., and VISHWANADHAM, N., 1985, Reliable Stabilization Using a Multi-Controller Configuration, *Automatica*, **21**, 599-602.

WALKER, B. K., 1980, A Semi-Markov Model Approach to Quantifying Fault Tolerant System Performance, Sc. D. dissertation, Dept. of Aero. and

Astro., M.I.T., Cambridge.

WALKER, B.K., 1983, Recent Developments in Fault Diagnosis and Accommodation, *AIAA Guidance and Control Conference*, Gatlinburg, Tennessee, AIAA-83-2258.

WILLSKY, A.S., 1976, A Survey of Design Methods for Failure Detection in Dynamic Systems, *Automatica*, **12**, 601-611.

WILLSKY, A.S., and JONES, H.L., 1976, A Generalized Likelihood Ratio Approach to the Detection and Estimation of Jumps in Linear Systems, *I.E.E.E. Trans. Autom. Control*, **21**, 108-112.

WONHAM, W.M., 1971, Random Differential Equations in Control Theory, in *Probabilistic Methods in Applied Mathematics*, Vol.2, edited by A.T. Bharucha-Reid , Academic Press, New York, 131-212.

YEDAVALLI, R.K., 1985, Perturbation Bounds for Robust Stability in Linear State Space Models, *Int. J. Control*, **42**, 1507-1517.

2.5 A Stochastically Stable FTCS Feedback Control Law

In this section, we derive a linear state feedback law for LTI FTCS and use the stochastic stability conditions derived in the previous subsection to analyze its stability for several different case. In particular, the necessary and sufficient conditions for LTI FTCS with linear state feedback are employed. As we show in the following manuscript, when the coupled matrix Riccati equations given in the last subsection have a finite steady state solution, almost sure asymptotic stability in probability is assured, and the simulation results we show in this subsection demonstrate this. When a finite steady state solution does not exist, then the system does not possess exponential stability in mean square, and again our simulation results show that divergence can occur.

We are in the process of running some extra simulations before submitting this manuscript for publication. Therefore, it should be treated as a draft version.

THE SYNTHESIS AND STABILITY OF A FEEDBACK CONTROL LAW FOR CONTINUOUS TIME FAULT TOLERANT CONTROL SYSTEMS

by

R. Srichander
Graduate Research Assistant

Bruce K. Walker
Associate Professor

Department of Aerospace Engineering & Engineering Mechanics
University of Cincinnati
Cincinnati, OH 45221-0343.

Tel: (513) 556-3552
FAX: (513) 556-4589

ABSTRACT

The synthesis of a feedback control law for active fault tolerant linear control systems is addressed in this paper. This synthesis technique is based on the use of a control model description of the system that closely resembles the actual system dynamics, which cannot be directly deduced due to random decision errors and delays by the failure detection and identification (FDI) system. The definition of stochastic stabilizability of active fault tolerant control systems and of the control model is introduced. Necessary and sufficient conditions for stochastic stabilizability of the control model are then established. These conditions lead to *necessary* conditions for the stochastic stabilizability of the class of active fault tolerant control systems examined. These conditions also provide the information necessary to construct an active fault tolerant feedback control law. The stochastic stability of the resulting closed loop system under this fault tolerant control law can then be examined by applying the necessary and sufficient conditions for exponential stability in the mean square derived in a companion paper. Finally, a numerical example is presented to illustrate the feedback control design methodology and to verify the results of the stability analysis.

1. INTRODUCTION

Active fault tolerant control involves detecting and identifying failures of the controlled system that occur at random instants of time and then compensating for these failures by some automatic logic. In particular, the control law must be reconfigured following the diagnosis of a failure by the automatic failure detection and identification (FDI) scheme. Because the FDI logic operates on measurement data corrupted by random noise and because the failure events to be diagnosed are random in nature, the FDI system is subject to random errors and delays. If the control design does not account for these errors and delays, catastrophic instability of the closed loop system can result, even if the system possesses deterministic closed loop stability for every failure mode that can be tolerated when the appropriate reconfigured control law is used.

In this paper, we consider the problem of synthesizing a fault tolerant control law for a linear system that is subject to actuator failures, and of verifying the stochastic stability of the resulting closed loop system (using the theory of (Srichander and Walker 1990)). The control synthesis and stability analysis techniques are developed such that the random failures of actuator components and the random errors and delays of the FDI system are accounted for. A numerical example of a simple fault tolerant system is used to demonstrate the control synthesis method and to illustrate the analysis of its closed loop stochastic stability.

In the remainder of this section, we will summarize the existing results relevant to control law design for systems subject to random mode changes, including active fault tolerant control systems.

The results that are relevant to our problem are those that involve the control of systems subject to random variations in the system parameters. Work on this topic dates back to Krasovskii and Lidskii (1961), who derived an optimal control law that minimizes an integral performance criterion for systems undergoing random structure variations (mode transitions) governed by a Markov process. The solution to this problem is based on the use of stochastic Lyapunov functions (Kushner 1967), the parameters of which are functions of the random process governing the structural changes. In (Krasovskii and Lidskii 1961), sufficient conditions for the optimality of this control law in minimizing a mean square error criterion are derived

assuming that an admissible control exists. The latter assumption ensures the boundedness of the cost function under the optimal control law.

Further investigations of the control problem for continuous time linear systems with structural parameters that randomly vary in a finite state space were carried out by Sworder (1969) and by Wonham (1971). In (Sworder 1969), the stochastic maximum principle is used to derive an optimal control law that minimizes an integral performance criterion function, while in (Wonham 1971), the dynamic programming principle is employed to arrive at a solution. In both cases, the optimal control law for a system with parameters governed by a jump Markov process is a state feedback control with gains that switch according to the state of the jump process. When the performance criterion of interest is quadratic, this class of problems leads to a jump linear quadratic regulator (JLQR) solution. In (Wonham 1971), sufficient conditions are also derived for the existence of a steady state optimal solution to the jump linear quadratic regulator problem based on the average transition rates between the modes and the stabilizability of the linear plant for each mode of the jump process.

In each of the formulations discussed above, it is assumed that the mode changes are correctly diagnosed immediately after they occur. In other words, it is assumed that the controller has knowledge of the true system description at every instant of time. The optimality of the resulting control law is guaranteed only under this restrictive assumption.

In practice, however, the mode changes must be identified using an FDI scheme. The behavior of these FDI schemes is statistical in nature due to the presence of measurement noise. Thus, the FDI system has nonzero error probabilities associated with its decisions and is subject to random decision delays. The likelihood of decision errors by FDI schemes can usually be reduced by increasing the time allowed for identifying a mode change. This modification, however, has the detrimental effect of increasing the average delay in detecting and responding to mode changes.

Under the delayed and imperfect decisions that are actually generated by the FDI scheme, the control law synthesis techniques discussed above do not even guarantee the stability of the unforced solution to the plant equations, let alone the optimality of the control law. Hence, any practical fault tolerant control design that reconfigures the control law based on FDI decisions must take into account the random detection delays and decision errors associated with those decisions to ensure the stability of the closed

loop system.

The design of active fault tolerant controllers that account for these effects to varying degrees have been investigated in (Caglayan *et al.* 1987), (Looze *et al.* 1984), (Looze, *et al.* 1985), and (Moerder *et al.* 1989). In (Looze *et al.* 1984), for instance, a reconfigurable control algorithm for a linear system based on the linear quadratic design methodology is presented. The algorithm uses the linear quadratic design parameters for the unfailed system as a basis for choosing the parameters for the failed system. Further, it is assumed that correct failure mode information is available to the controller at all times except for imprecise knowledge of the remaining control effectiveness. The validity of this assumption is questionable in practice, particularly when analytic redundancy techniques are used for FDI (Horak, 1988) In (Moerder *et al.* 1989), the feedback gains for the no-fail and control-impaired cases are designed off-line and scheduled as a function of the FDI information. Again, the assumption that the FDI logic requires only a short delay before correctly identifying the failure mode renders the technique inapplicable for many practical systems.

In each of the references cited above, the choice of the control law is based on deterministic stability analysis of the resulting closed loop system for those cases where the FDI scheme has correctly identified the failure modes. Clearly, under random parametric variations in the given system and random detection delays and errors by the FDI scheme, the resulting system is actually governed by stochastic differential equations. Hence, the stability conclusions of the references above are suspect. This will be demonstrated later in this paper by a numerical example.

In this paper, we present a control synthesis technique that yields a fault tolerant feedback control law that explicitly accounts for the random decision errors and delays associated with the FDI process.

The rest of the paper is organized as follows: In section 2, we will formulate the fault tolerant control problem and introduce a *control model* for the system dynamics. Then, we derive an optimal control law that minimizes a given performance index for the control model. The definition of stochastic stabilizability is also given in this section. The results are then used in section 3 to derive *necessary* conditions for stabilizability of the plant. In section 4, a synthesis method for a fault tolerant control law for the actual plant is presented, which makes use of the information provided by the stabilizability conditions. The stability analysis of the

plant under this control law is then addressed using the results in (Srichander and Walker 1990). The control design methodology and the stability analysis are then illustrated by a numerical example in section 5. Conclusions are summarized in section 6.

2. PROBLEM FORMULATION AND THE CONTROL MODEL

The stochastic evolution of the systems of interest in this paper are characterized by two random processes, one describing the mode jumps occurring in the system description (which represent the failures), and the other describing the FDI process that monitors these random parametric jumps. The linear plant model is assumed to be described by:

$$\dot{x}(t) = Ax(t) + B(\eta)u(x,r,t) \tag{2.1}$$

where $u(x,r,t)=-K(r)x(t)$. In (2.1), $\eta(t)$ is a continuous time, discrete state Markov process modeling the failures occurring in the system and takes values in the finite set $\mathbf{Z}=\{1,2,..,\nu\}$. In (2.1), $r(t)$ is also a continuous time, discrete state Markov process that models the FDI process and takes values in the set $\mathbf{S}=\{1,2,..,\gamma\}$. We will assume that α_{ij} $(i,j\in\mathbf{Z})$ represents the transition rates of the failure process $\eta(t)$ (i.e. the failure rates) and q_{ij}^{k} $(i,j\in\mathbf{S},\ k\in\mathbf{Z})$ represents the conditional transition rates of the FDI process $r(t)$ given that $\eta(t)=k$ (i.e. the rates of FDI decisions). The rates α_{ij} and q_{ij}^{k} are assumed to be known. $x(t)\in\mathbb{R}^n$ is the process state vector and $u(x,r,t)\in\mathbb{R}^m$ is the control vector, which is explicitly constrained to be dependent only on the process state vector $x(t)$ and the state of the FDI process $r(t)$. In other words, the control is *not* allowed to depend on the true failure state $\eta(t)$, which is known only indirectly through the FDI state $r(t)$. We will also assume that $u(x,r,t)$ takes the linear state feedback form $u(x,r,t)=-K(r)x(t)$, which will be shown later in this paper to be the form of the globally optimal feedback control law for a quadratic cost problem related to the problem at hand.

Note that (2.1) restricts the effects of failures to the input sensitivity matrix B. The results derived here, however, extend directly to the case where the system dynamics matrix A is affected by the failure. Also, nonzero bias terms that are dependent on η can be added to (2.1) if the results are suitably modified. For brevity, we will present complete results only for the restricted case described by (2.1).

The synthesis of a fault tolerant feedback control law $u(x,r,t)=-K(r)x(t)$, $r\in\mathbf{S}$ for the plant model (2.1) is the main focus of this paper. We will also establish necessary conditions for the existence of a fault tolerant control law of this feedback form that stochastically stabilizes the plant (2.1) (i.e. necessary conditions for stochastic stabilizability). These conditions will be seen later to relate directly to the information needed to construct the control gain matrix $K(r)$.

In order to derive necessary conditions for stochastic stabilizability of the plant model (2.1), we introduce the following *control model* description:

$$\dot{\bar{x}}(t) = A\bar{x}(t) + B(\eta)\bar{u}(\bar{x},r,\eta,t) \qquad (2.2)$$

Obviously, the control model (2.2) differs from the plant model (2.1) in the form of the control law. For the control model (2.2), we assume that the control law $\bar{u}(\cdot)$ is a function of the system states $\bar{x}(t)$, the FDI process state $r(t)$, and the failure process state $\eta(t)$. In other words, we assume in (2.2) that we can design a fictitious controller that uses information on *both* of the Markovian processes $r(t)$ and $\eta(t)$. As noted above, the state of the failure process $\eta(t)$ is not available to the controller in practice. However, our objective here is to solve an optimization problem for the control model (2.2), which then will help us to derive necessary conditions for stochastic stabilizability of the plant model (2.1) and to construct a control law for the plant (2.1) that results in a stable closed loop system.

In deriving the optimal control law $\bar{u}^*(\cdot)$ for the control model (2.2), we specify that any control law $\bar{u}(\cdot)$ that uses information from the failure process state $\eta(t)$ *only* and disregards the information provided by the FDI process state $r(t)$ is *not* an *admissible* control law. In other words, if Φ denotes the class of admissible controls for the control model (2.2), then Φ: $t\times\mathbb{R}^n\times\mathbf{S}\times\mathbf{Z}\rightarrow\mathbb{R}^m$ or Φ: $t\times\mathbb{R}^n\times\mathbf{S}\rightarrow\mathbb{R}^m$. This assumption is consistent with the nature of the fault tolerant control problem, where only information from the FDI process state $r(t)$ is available in practice. Notice that if the FDI and failure process states are the same at every instant of time (as is the case under the assumption of instantaneous correct diagnosis of the failure mode by the FDI process), then the plant model (2.1) and the control model (2.2) are identical (each breaking down to the Markovian jump system

considered in (Ji and Chizeck 1990)).

Before we derive the optimal control law $\bar{u}^*(\cdot)\in\Phi$ for the control model (2.2), we will define stochastic stabilizability with reference to the plant model (2.1) and the control model (2.2).

Definition 2.1: The plant model (2.1) is said to be *stochastically stabilizable* if, for any $x_0\in\mathbb{R}^n$, $r_0\in\mathbf{S}$, and $\eta_0\in\mathbf{Z}$, there exists a linear state feedback control law $u(x,r,t)=-K(r)x(t)$ such that for any bounded positive definite matrix $M(r,\eta)$ (possibly time varying) which is a function of the FDI and failure process states, the solution $x(t)$ of (2.1) satisfies the following inequality for some bounded $\tilde{M}>0$:

$$\lim_{T\to\infty} E\left\{\int_{t_0}^{T} x^T(t)M(r,\eta)x(t)dt\right\} \le x_0^T\tilde{M}x_0 \qquad (2.3)$$

(We will call a $m\times n$ matrix bounded if there exists a positive constant β such that $\|Ax\|\le\beta\|x\|$ $\forall x\in\mathbb{R}^n$, $x\neq 0$. Here $\|x\|=(x_1^2+x_2^2+\ldots+x_n^2)^{1/2}$ where x_i are the components of $x\in\mathbb{R}^n$).

It is easy to see that under the above definition, stochastic stabilizability of the plant model (2.1) implies that there exists a feedback control law $u(x,r,t)=-K(r)x(t)$, $r\in\mathbf{S}$ which drives the state $x(t)$ from any given initial condition $x_0\in\mathbb{R}^n$ asymptotically to the origin in the mean square sense given any initial conditions $r_0\in\mathbf{S}$ and $\eta_0\in\mathbf{Z}$ on the FDI and failure process states.

Definition 2.2: The control model (2.2) is said to be stochastically stabilizable if, for any $\bar{x}_0\in\mathbb{R}^n$, $r_0\in\mathbf{S}$, and $\eta_0\in\mathbf{Z}$, there exists an *admissible* state feedback control law $\bar{u}(\bar{x},r,\eta,t)=-K(r,\eta)\bar{x}(t)$ such that for any bounded positive definite matrix $M(r,\eta)$ (possibly time varying) which is a function of the FDI and failure process states, the solution $\bar{x}(t)$ of (2.2) satisfies the following inequality for some bounded $\tilde{M}>0$:

$$\lim_{T\to\infty} E\left\{\int_{t_0}^{T} \bar{x}^T(t)M(r,\eta)\bar{x}(t)dt\right\} \le \bar{x}_0^T\tilde{M}\bar{x}_0 \qquad (2.4)$$

The stochastic stabilizability of (2.2) implies that there exists a

feedback control law $\bar{u}(\bar{x}, r, \eta, t) = -K(r, \eta)\bar{x}(t)$, $r \in S$ and $\eta \in Z$ among the class of admissible controls Φ, which drives the state $\bar{x}(t)$ of (2.2) from any given initial condition $\bar{x}_0 \in \mathbb{R}^n$ asymptotically to the origin in the mean square sense given any initial conditions $r_0 \in S$ and $\eta_0 \in Z$ on the FDI and failure process states.

We will now derive an optimal control law for the control model (2.2) that minimizes a particular performance index. This will then enable us to derive stabilizability conditions for the plant (2.1), which in turn will lead to a control law for the plant (2.1). The notation used in the discussion to follow will be the same as that used in (Srichander and Walker 1990). In particular, the operator $\mathcal{L}$ will denote the weak infinitesimal operator of the (n+2)-dimensional jointly Markov process $\{\bar{x}, r, \eta\}$.

Consider the following index of performance,

$$J = E\left\{\int_{t_0}^{T} L(\bar{x}, r, \eta, \bar{u}, t)dt\right\} \tag{2.5}$$

where $L(\cdot)$ is a positive definite function. Let us consider the function $V(\bar{x}, r, \eta, t)$ that satisfies the functional equation

$$V(\bar{x}, r, \eta, t) = \min_{\bar{u} \in \Phi} E\left\{\int_{t}^{T} L(\bar{x}, r, \eta, \bar{u}, t)dt \,\middle|\, \bar{x}(t), r(t), \eta(t)\right\} \tag{2.6}$$

Then the following theorem holds.

Theorem 2.1: The optimal control $\bar{u}^*(\cdot) \in \Phi$ for the control model (2.2) that minimizes (2.5) is the solution to Bellman's equation,

$$\min_{\bar{u} \in \Phi} \left[\mathcal{L}V(\bar{x}, r, \eta, t) + L(\bar{x}, r, \eta, \bar{u}, t)\right] = 0 \tag{2.7}$$

subject to the boundary condition,

$$V(\bar{x}(T), r(T), \eta(T), T) = 0 \tag{2.8}$$

The proof for this theorem follows similar lines to those used in (Wonham 1971) for deriving an optimal control law for the Markovian jump system with perfect information structure.

In particular now, let us consider the positive definite quadratic function

$$L(\bar{x}, r, \eta, \bar{u}, t) = \bar{x}^T Q(r,\eta)\bar{x} + \bar{u}^T(\cdot)R(r,\eta)\bar{u}(\cdot), \quad r\in S, \quad \eta\in Z \tag{2.9}$$

where $Q(r,\eta)>0$, $R(r,\eta)>0$ $\forall r\in S$ and $\forall\eta\in Z$. Further, let us assume $V(\bar{x}, r, \eta, t)$ is the quadratic function $V(\bar{x}, r, \eta, t)=\bar{x}^T\bar{P}(r,\eta,t)\bar{x}$. We shall denote $Q(r,\eta)=Q_{ik}$, $R(r,\eta)=R_{ik}$, $\bar{P}(r,\eta,t)=\bar{P}_{ik}(t)$ and $\bar{u}(x,r,\eta,t)=\bar{u}_{ik}(t)$, when $r=i\in S$ and $\eta=k\in Z$.

Evaluating $\mathcal{L}V(\bar{x}, r, \eta, t)$ for the control model (2.2) when the quantities $r=i\in S$ and $\eta=k\in Z$ have occurred at time t, we have

$$\begin{aligned}\mathcal{L}V = \bar{x}^T\Big[&\dot{\bar{P}}_{ik}(t) + A^T\bar{P}_{ik}(t) + \bar{P}_{ik}(t)A + \sum_{\substack{j\in S\\ j\neq i}} q_{ij}^k(\bar{P}_{jk}(t)-\bar{P}_{ik}(t)) \\ &+ \sum_{\substack{j\in Z\\ j\neq k}} \alpha_{kj}(\bar{P}_{ij}(t)-\bar{P}_{ik}(t))\Big]\bar{x} + \bar{x}^T\bar{P}_{ik}(t)B_k\bar{u}_{ik}(t) \\ &+ \bar{u}_{ik}^T(t)B_k^T\bar{P}_{ik}(t)\bar{x}, \quad i\in S, \quad k\in Z\end{aligned} \tag{2.10}$$

It can be easily shown that the minimization in (2.7) using (2.9) and (2.10) gives,

$$\bar{u}_{ik}^*(t) = -R_{ik}^{-1}B_k^T\bar{P}_{ik}(t)\bar{x}(t), \quad i\in S, \quad k\in Z \tag{2.11a}$$

$$= -K_{ik}^*(t)\bar{x}(t), \quad i\in S, \quad k\in Z \tag{2.11b}$$

where the $\bar{P}_{ik}(t)$, $i\in S$, $k\in Z$, solve the coupled matrix Riccati equations,

$$\begin{aligned}&\dot{\bar{P}}_{ik}(t) + \tilde{A}_{ik}^T\bar{P}_{ik}(t) + \bar{P}_{ik}(t)\tilde{A}_{ik} + \sum_{\substack{j\in S\\ j\neq i}} q_{ij}^k\bar{P}_{jk}(t) + \sum_{\substack{j\in Z\\ j\neq k}} \alpha_{kj}\bar{P}_{ij}(t) \\ &+ K_{ik}^{*T}(t)R_{ik}K_{ik}^*(t) + Q_{ik} = 0, \quad i\in S, \quad k\in Z\end{aligned} \tag{2.12}$$

with boundary conditions,

$$\bar{P}_{ik}(T) = 0, \quad \forall i\in S, \quad \forall k\in Z \tag{2.13}$$

In (2.12), $\tilde{A}_{ik}(t)$ is defined as

$$\tilde{A}_{ik}(t) = A - B_k K^*_{ik}(t) - 0.5 \sum_{\substack{j\in S \\ j\neq i}} q^k_{ij} - 0.5 \sum_{\substack{j\in Z \\ j\neq k}} \alpha_{kj}, \quad i\in S, \; k\in Z \tag{2.14}$$

The coupled Riccati equations given by (2.12) have identical structure to the coupled Riccati equations derived by Wonham (1971). Hence, under the boundary conditions (2.13), these equations can be solved by quasi-linearization and the successive approximation technique given in (Wonham 1971). We shall assume without loss of generality (because both the plant and the control model are time invariant systems) that T=0 and $t_0=-\infty$ in (2.5). It follows from (Wonham 1971) then that the solutions to (2.12) with the boundary conditions (2.13) are unique, non-negative definite and monotonically increasing as $t\to-\infty$. Further, the assumption that $Q_{ik}>0$ implies $\bar{P}_{ik}(t)>0$ for $i\in S$, $\eta\in Z$ and $\forall t\geq 0$. Therefore, the control law given by (2.11) is the unique optimal control for this quadratic cost function, and it has the state feedback form that we hypothesized earlier.

Let us assume that as $t\to-\infty$ there exist steady state solutions $\bar{P}_{ik}>0$, $\forall i\in S$ and $\forall k\in Z$ to the coupled Riccati equations (2.12) with the boundary conditions (2.13). Then it follows from (2.6) that the minimum cost under the control law (2.11) is given by,

$$J_{min} = \bar{x}_0^T \bar{P}_{r_0\eta_0} \bar{x}_0 \tag{2.15}$$

For any other admissible control law $\bar{u}(\cdot)\in\Phi$ for the control model (2.2), the cost incurred for the performance index (2.5) is greater than J_{min}. Now, let us consider the case where the controller has information only on the FDI process state r(t). Under the assumption that $\eta(t)=r(t)=i\in S$ and that S=Z, the optimal control law (2.11) becomes,

$$\bar{u}^*(x, r=i, \eta=i, t) = -K^*_{ii}(t)\bar{x}(t), \quad i\in S \tag{2.16}$$

So, a natural restriction to make to the optimal control law (2.11) in order to arrive at a control law that depends only upon the FDI state r(t) is to use the control law:

$$\bar{u}(\bar{x}, r, t) = \bar{u}^*(\bar{x}, r, \eta, t)\big|_{\eta=r} = -K^*_{ii}(t)\bar{x}(t) \text{ when } r=i \qquad (2.17)$$

This will lead later to a control law for the plant (2.1) without the assumption that S=Z. Let us denote by J the cost incurred under the control law (2.17) for the control model (2.2). Then $J \geq J_{min}$, the equality sign applying when mode changes of the failure process are instantaneously detected.

The next section gives conditions for stochastic stabilizability of the control model (2.2) and the plant model (2.1). These conditions will ultimately lead to a control law for the plant model (2.1) that is similar to the restricted control law (2.17).

3. CONDITIONS FOR STOCHASTIC STABILIZABILITY

The following theorem gives conditions for the stochastic stabilizability of the control model (2.2).

Theorem 3.1: The control model (2.2) is stochastically stabilizable if and only if there exist steady state solutions $\{\bar{P}_{ik} > 0,\ i \in S,\ k \in Z\}$ to the coupled Riccati equations (2.12) under the boundary conditions (2.13) for any $Q_{ik} > 0$, $R_{ik} > 0$ $\forall i \in S$ and $\forall k \in Z$.

The proof of this theorem is given in the Appendix. Notice that the conditions for the stochastic stabilizability of the control model (2.2) given by Theorem 3.1 are very easy to check by numerically solving (2.12), as opposed to the conditions for stochastic stabilizability of the jump linear quadratic regulator problem derived by Ji and Chizeck (1990), which cannot be checked in practice.

Necessary conditions for stochastic stabilizability of the plant model (2.1) are given by the following theorem:

Theorem 3.2: Necessary conditions for stochastic stabilizability of the plant model (2.1) are that there exist steady state solutions $\{\bar{P}_{ik} > 0,\ i \in S,\ k \in Z\}$ to the coupled Riccati equations given by (2.12) under the boundary conditions (2.13).

Proof:

Let us assume that steady state solutions $\{\bar{P}_{ik}>0,\ i\in S,\ k\in Z\}$ *do not* exist to the coupled Riccati equations given by (2.12). Then, it follows from Theorem 3.1 that no admissible control law of the form $\bar{u}(x,r,\eta,t)=-K(r,\eta)\bar{x}(t)$, $r\in S$ and $\eta\in Z$ exists for the control model (2.2) such that condition (2.4) is satisfied. We need to show that under the above assumption there exists no control law of the form $u(x,r,t)=-K(r)x(t)$, $r\in S$ to the plant model (2.1) that satisfies the condition (2.3). We shall show this by contradiction.

Suppose that when steady state solutions $\{\bar{P}_{ik}>0,\ i\in S,\ k\in Z\}$ *do not* exist to the coupled Riccati equations (2.12) under the boundary conditions (2.13), a control law of the form $u(x,r,t)=-K(r)x(t)$, $r\in S$, exists for the plant (2.1) such that condition (2.3) is satisfied. Now, consider the following control law for the control model (2.2):

$$\bar{u}(x,r,\eta,t) = -K(r)\bar{x}(t),\ r\in S \tag{3.1}$$

The above control law uses information only from the FDI process r(t) (and hence is a restricted information control law), but nevertheless belongs to the class of admissible controls Φ. Using the control law (3.1), it is easy to see that the plant model (2.1) and the control model (2.2) become identical. This implies that the solutions x(t) to (2.1) and $\bar{x}(t)$ to (2.2) respectively are such that $x(t)=\bar{x}(t)\ \forall t\geq t_0$ provided $\bar{x}_0=x_0$. Since the control law $u(x,r,t)=-K(r)x(t)$ for the plant (2.1) satisfies condition (2.3) by hypothesis, it follows immediately that the condition (2.4) is also satisfied under the control law (3.1) for the control model (2.2). In other words, the control model (2.2) is stochastically stabilizable when steady state solutions $\{\bar{P}_{ik}>0,\ i\in S,\ k\in Z\}$ do not exist to (2.12). But this contradicts Theorem 3.1, and this proves the theorem.

Note that the conditions to be checked in Theorem 3.2 are identical to those in Theorem 3.1, namely the existence of steady state solutions $\bar{P}_{ik}$, $i\in S$ and $\eta\in Z$ to the coupled Riccati equations (2.12) with boundary conditions (2.13).

4. CONTROL LAW SYNTHESIS AND STABILITY ANALYSIS

Theorem 3.2 is very useful for determining whether it is possible to

synthesize a feedback control law for the plant model (2.1) that will lead to a stochastically stable closed loop system. The non-existence of steady state solutions $\{\bar{P}_{ik}>0,\ i\in S,\ k\in Z\}$ to (2.12) under the boundary conditions (2.13) implies that *no* linear feedback control law $u(\cdot)= -K(r)x(t),\ r\in S$ can stochastically stabilize the plant model (2.1). Under these conditions, a fault tolerant control system designer has no choice but to try to redesign the FDI algorithm such that the transition rates of the modified FDI process r(t) lead to the existence of steady state solutions $\{\bar{P}_{ik}>0,\ i\in S,\ k\in Z\}$ to the coupled Riccati equations. If no such FDI redesign can be found, then the designer must admit defeat and seek a complete redefinition of the system specifications because stochastic stability of the feedback system is not possible.

Assuming the conditions for stochastic stabilizability of the plant (2.1) are satisfied, we will indicate below a synthesis of a feedback control law for the plant model (2.1) that accounts for the transition rates of the FDI and failure processes in its design. We will refer to this control law as a fault tolerant control law for the plant model (2.1). The closed loop stochastic stability of the plant model (2.1) under this control law can then be examined using the results in (Srichander and Walker 1990), which will be stated later in this paper.

4.1 Feedback control law synthesis.

Let us consider the optimal control law (2.11) that minimizes the performance index (2.5) for the control model (2.2). This control law uses information from both the failure process and the FDI process to ensure optimality of the given cost function. The steady state optimal control law for (2.2) when $r=i\in S$ and $\eta=k\in Z$ will be denoted by $\bar{u}(\bar{x},r,\eta)=-\bar{K}^{*}_{ik}\bar{x}(t)$.

In synthesizing a feedback control law for the plant model (2.1), the controller has access only to the FDI process state r(t). In practice, the FDI scheme is designed with the intent that the FDI process state r(t) should follow the failure process state $\eta(t)$ as closely as possible. With this in mind, a reasonable choice for a control law for the plant (2.1) is to assume that $\eta(t)=r(t)$ in the control law (2.11), just as we did in establishing the restricted control law given by (2.17), which was restricted to the case where S=Z. Following this argument, we will choose the fault tolerant control law based on the following logic.

(i) *When FDI and failure processes have identical state spaces (i.e. S=Z)*:
When the FDI scheme indicates $r=i\in S$, the fault tolerant control law $u(x,r,t)\equiv u_i$ will be chosen as:

$$u_i = -R_{ii}^{-1}B_i^T\bar{P}_{ii}x(t) = -K_{ii}^{*}x(i) = -K_i x, \quad i\in S \tag{4.1}$$

exactly as in (2.17).

(ii) *When FDI and failure processes have different state spaces*:
Assume that $Z\subset S$. This implies that the FDI process can have additional states relative to the failure process. This is common because additional FDI process states are often necessary to represent intermediate FDI conditions, such as the detection of a failure but without isolation. Let us assume that the Z is arranged such that when η takes increasing values in the set $Z\equiv\{1,2,..,\nu\}$, the system operation is more degraded. Similarly, let S be arranged such that when r takes increasing values from the set $S\equiv\{1,2,..,\gamma\}$, the FDI scheme indicates greater degradation in the system operation. In this case, the following fault tolerant control law will be chosen for (2.1) when $r=i\in S$:

(a) When $r=i\in Z$, then u_i is chosen as in (4.1).

(b) When $r=i\notin Z$, then select

$$u_i = \frac{1}{2}\left(u_{i-a}+u_{i+b}\right), \quad i\in S \tag{4.2}$$

where a and b are positive integers such that $\min_a(i-a)\in Z$ and $\min_b(i+b)\in Z$. Thus, the control is selected as the average of the control for the failure state for which FDI process state i is the appropriate FDI state and the control for the next level of degradation of the failure process. Other strategies could also be used for selecting the control, but this strategy has the advantage that it incorporates some "hedging" against the next possible level of degradation.

4.2 Stability analysis.

The closed loop stochastic stability of the plant model (2.1) under the fault tolerant control law $u_i=-K_i x$, $i\in S$, given by (4.1) and (4.2) can be investigated by applying Theorem 5.1 of (Srichander and Walker 1990). This

theorem is restated below:

Theorem 4.1 (Srichander and Walker 1990): A necessary and sufficient condition for exponential stability in the mean square of the linear plant model (2.1) under the control law $u_i=-K_i x$, $i\in S$, given by (4.1) and (4.2) is that there exist finite steady state solutions $\{P_{ik}>0,\ i\in S,\ k\in Z\}$ as $t\to-\infty$ to the following coupled linear matrix differential equations:

$$\dot{P}_{ik}(t) + \tilde{A}_{ik}^T P_{ik}(t) + P_{ik}(t)\tilde{A}_{ik} + \sum_{\substack{j\in S \\ j\neq i}} q_{ij}^k P_{jk}(t)$$

$$+ \sum_{\substack{j\in Z \\ j\neq k}} \alpha_{kj} P_{ij}(t) + Q_{ik} = 0,\ i\in S,\ k\in Z,\ t\in(-\infty,0] \qquad (4.3)$$

with boundary conditions,

$$P_{ik}(0) = 0,\ \forall i\in S,\ \forall k\in Z \qquad (4.4)$$

where $Q_{ik}>0$, $\forall i\in S$, $\forall k\in Z$, and

$$\tilde{A}_{ik} = A - B_k K_i - 0.5 \sum_{\substack{j\in S \\ j\neq i}} q_{ij}^k - 0.5 \sum_{\substack{j\in Z \\ j\neq k}} \alpha_{jk},\ i\in S,\ k\in Z \qquad (4.5)$$

Note that the linear matrix equations given by (4.3) and (4.5) differ from the matrix Riccati equations given by (2.12) in the value of the feedback gain K that appears in the terms. Therefore, the Riccati equations represented by (2.12) must be solved first to establish the possible stochastic stabilizability (or the lack thereof) of (2.1) and to synthesize the control law (4.1) and (4.2). Then, the equations (4.3) can be solved to determine whether the resulting closed loop system possesses stochastic stability.

Note also that Theorem 4.1 states *necessary and sufficient* conditions for stochastic stability of the closed loop plant. Thus, checking these conditions leads to a definite conclusion regarding the stochastic stability of the closed loop plant.

We will now illustrate the above fault tolerant control law design methodology and stability analysis for the plant model (2.1) with a

numerical example. Numerical simulation results for the resulting closed loop system will then be presented to verify the Theorem 4.1.

5. NUMERICAL RESULTS

To illustrate the design methodology for active fault tolerant control systems presented above and the stability conditions derived in (Srichander and Walker 1990), we will consider a first order system with two possible modes of operation, i.e. $Z=\{1,2\}$ where $\eta=1$ represents a "normal" system and $\eta=2$ represents a "degraded" system with Markovian transitions for the failure process $\eta(t)$. We assume that the FDI process intended to detect these mode changes uses single sample tests on a test statistic that is corrupted by additive white noise. Therefore, the FDI process state r(t) is also Markovian with the same two states ($S=Z=\{1,2\}$). The following numerical parameters are used for this example:

$A=0.4$ (hence, the open loop system is unstable),

$B_1=1.0$, $B_2=0.2$, $\alpha_{12}=0.005$, $\alpha_{21}=0.001$.

Thus, a "degraded" system has only 20% of the control effectiveness of a "normal" system. Such a loss occurs every 200 time steps on average, and the system is capable of "self-healing", but the average time to self-heal is 1000 time steps.

We will assume that the FDI test statistic examined at each time step is $N(0,1)$ under normal conditions ($\eta=1$) and $N(1,1)$ under degraded conditions ($\eta=2$). Here, $N(a,\sigma^2)$ represents a normal distribution with mean a and variance σ^2. The threshold for this test is denoted T_1.

We shall further assume that there is a second test which is intended to recover from false degradation indications by the FDI scheme. These tests are frequently used in practice to recover from false alarms, and such a test is apprpriate in this example in light of the system's capability to self-heal. The test statistic for this test will be assumed to be $N(0,1)$ when a degraded system is under test and $N(1,1)$ when the system is normal. The threshold for this test is T_2.

Both FDI tests are assumed to be performed at a rate of 5 Hz.

We shall illustrate below the synthesis of a fault tolerant control law for the above example for several different FDI transition rates, which are determined by the thresholds T_1 and T_2. We shall also examine the stochastic

stability of the solution x=0 of (2.1) under the control law that results from using (4.1) and (2.12). In all cases, the computation of $P_{ik}(t)$, $i \in \mathbf{S}$ and $k \in \mathbf{Z}$ in (4.3) and of $\bar{P}_{ik}(t)$ in (2.12) was truncated after 200 secs (1000 time steps), which should be sufficient time to indicate convergence of the solutions to a steady state or nonconvergence.

Case (1)

Let us assume that the thresholds for the FDI scheme are $T_1=1.8$ and $T_2=2.0$. It is easy to calculate that under these conditions the FDI transition rates are,

$$q^1_{12}=0.18,\ q^2_{12}=1.06,\ q^1_{21}=0.79,\ q^2_{21}=0.12$$

Note that correct detections are nearly 6 times more likely than false alarms and recoveries from false alarms are more than 6 times more likely than continued false isolations. These behaviors are not uncommon in practice.

In synthesizing the fault tolerant control law, the following parameters are assumed for the quadratic cost (2.9):

$$R_{ik}=1.0,\ \forall i \in \mathbf{S},\ \forall k \in \mathbf{Z}$$

$$Q_{11}=1.0,\ Q_{12}=0.5,\ Q_{21}=1.75,\ Q_{22}=1.0$$

The following state feedback gains are obtained for the fault tolerant control law using the design methodology given in section 4.1:

$$K_1=1.538,\ K_2=4.225$$

The closed loop system then has the following deterministic stability characteristics under each combination of η and r:

η	r	A - B(η)K(r)	
1	1	-1.138	Stable under normal conditions.
1	2	-4.625	Stable following false alarm.
2	1	0.093	*Unstable* with undetected failure.
2	2	-0.445	Stable following correct detection.

It is worthy of note that this system does *not* possess deterministic stability for one of the two cases where the FDI process state does not correctly indicate the failure process state. Most of the previously reported efforts to design reconfigurable control laws would accept this control law as satisfactory despite this instability because the closed loop system is deterministically stable for both cases where η=r. As we shall see below, however, the stochastic stability of this system must be carefully examined when FDI errors and delays can lead to periods when η and r differ.

The stochastic stability of the closed loop plant using the above parameters can be investigated by applying Theorem 4.1. We will assume that Q_{ik}=1.0, $\forall i \in S$, $\forall k \in Z$ in the linear matrix equations (4.3). Note that these are not the values of Q_{ik} given in the cost function. However, Theorem 4.1 does not require that the linear matrix equations have a finite steady state solution for just the given Q_{ik} but rather for *any* Q_{ik} such that $Q_{ik}>0$ $\forall i \in S$ and $\forall k \in Z$. Therefore, Q_{ik}=1.0 $\forall i \in Z$ and $\forall k \in S$ is reasonable for solving (4.3) in order to check the stochastic stability conditions.

A summary of the results for this case is given in Table 1. The equations (4.3) under the boundary conditions (4.4) have steady state solutions for the thresholds and gains chosen here. From Theorem 4.1, we infer that this condition implies that the solution x=0 of (2.1) is exponentially stable in the mean square. Further, from the remarks on Theorem 5.1 in (Srichander and Walker, 1990), this implies that the solution x=0 of the plant model (2.1) is almost surely asymptotically stable in probability. In light of the deterministic stability properties for this system discussed above, we see that the system can "tolerate intermittent intervals of instability" and still possess stochastic stability of a relatively strict kind.

To verify these conclusions, a numerical simulation of the linear plant using the thresholds and gains in Table 1 was carried out for a duration of 100 secs (or 5000 time steps). This is sufficiently long for an average of 25 degradations or 5 self-healings to occur.
The occurrence of
failure process transitions was randomly triggered by checking the value at each point of time of a pseudorandom number uniformly distributed between zero and unity against α_{12} or α_{21}, depending on whether the state of the failure process η at that time point was 1 or 2, respectively.

order to
investigate the behavior
of the FDI scheme and the control law when a failure is present. Fig.1 shows one representative sample
function observed for this case. It is seen from Fig.1 that the solution x=0 of (2.1) observed is asymptotically stable, which in turn agrees with the analytical results in section 5 of the accompanying paper (Srichander and Walker 1990).

Case (2)

For the second case, we shall assume that the FDI thresholds are T_1=1.2 and T_2=0.8. This changes the transition rates of the FDI process from those considered for case (1). The FDI test statistic is assumed to have the same distribution function as in case (1). In synthesizing a fault tolerant control law along the lines of section 3.1, the following parameters were selected for the cost function.

$$R_{ik}=1.0, \ \forall i\in S, \ \forall k\in Z$$

$$Q_{11}=1.0, \ Q_{12}=2.0, \ Q_{21}=0.5, \ Q_{22}=1.5$$

Table 2 lists the various parameters obtained for this case. Again, steady state solutions to equation (4.3) were obtained for the selected design parameters. This implies that the solution x=0 of (2.1) is almost surely asymptotically stable. One sample function from a numerical simulation of the plant model (2.1) for the above parameters with a forced mode transition from state 1 to state 2 at t=5 secs is given in Fig.2. Again, we can see that the simulation result agrees with the stability results predicted in the accompanying paper (Srichander and Walker 1990).

Case (3)

For this case, the FDI thresholds and test statistics are assumed to be the same as in case (2), but the gains K_1 and K_2 are chosen arbitrarily. These gains ensure stability of the deterministic closed loop system when $r=\eta$. In this case, the solutions $\{P_{ik}(t), \ i\in S, \ k\in Z\}$ to equation (4.3) under the boundary conditions (4.4) are unbounded as $t\to-\infty$, indicating that the plant model under the above control law lacks stability in the exponential mean square sense. The design parameters are summarized in Table 3. Again, one representative sample function observed during the simulation run is shown in Fig.3. It is easy to see that this sample function lacks exponential stability.

Cases (4) & (5)

Two other cases were examined to illustrate the importance of accounting for the FDI transition rates while synthesizing a fault tolerant control law for the plant model to ensure stochastic stability. For case (4), the thresholds are chosen as T_1=3.0 and T_2=1.5, while the gains are selected as K_1=1.4 and K_2=2.25. For these design parameters, it follows from Theorem 4.1 that the plant model lacks exponential stability in the mean square. A representative sample function observed during the simulation run is is shown in Fig.4.

In case (5), identical gains K_1 and K_2 are used, but the thresholds are chosen as T_1=1.8 and T_2=2.0. For these parameters, the solutions $\{P_{ik}(t), i\in S, k\in Z\}$ to (4.3) under the boundary conditions (4.4) have a steady state solution. This implies that the plant model (2.1) for the above design parameter values is almost surely asymptotically stable. One sample function observed during the simulation is shown in Fig.5. This sample function can be seen to have asymptotic stability. The design parameters for this case are summarized in Table 5.

Before concluding this section, the following comments on the numerical results are in order: We first note that the gains chosen in each case study ensure stability of the deterministic closed loop system when $r=\eta$. Under incorrect decisions by the FDI scheme, we see from the simulations that for two of the cases investigated, the solutions go unbounded as time increases. In particular, cases (4) and (5) use the same gains K_1 and K_2 with *different transition rates* for the FDI process. But the sample solution observed for case (4) is not bounded as time increases. This representative example illustrates the importance of accounting for the FDI process transition rates in synthesizing a control law for fault tolerant control systems that use FDI information for reconfiguring the control gains.

The reconfigurable control methodologies that have been investigated in the literature (Caglayan *et al.* 1987, Looze *et al.* 1984, 1985 and Moerder *et al.* 1989) do not account for the FDI transition rates in either deriving the control laws or in addressing the stability of the resulting closed loop system. Hence, when incorrect decisions by the FDI scheme are possible, the stability of the resulting closed loop system is suspect. The numerical examples presented in this section verify this claim.

6. CONCLUSIONS

The synthesis of a fault tolerant control law for the plant model (2.1) that takes into account the transition rates of both the FDI and failure

processes was developed. The necessary conditions for stochastic stabilizability of the plant model were also derived. These conditions are easy to check, and hence are useful tools for the fault tolerant control designer. A numerical example was presented to illustrate the design methodology presented here. The importance of accounting for the FDI transition rates in synthesizing a feedback control law for the plant model was clearly brought out through the simulation results.

APPENDIX

Proof of Theorem 3.1:

Let us assume that steady state solutions $\{\bar{P}_{ik}>0,\ i\in S,\ k\in Z\}$ exist to the coupled Riccati equations (2.12) under the boundary conditions (2.13) for any $Q_{ik}>0$, $R_{ik}>0$, $\forall i\in S$ and $\forall k\in Z$. Choosing the control law $\bar{u}(\cdot)$ for (2.2) as in (2.11), it follows that the cost function (2.5) under this control law incurs the minimum cost given by (2.15) among all admissible controls $\bar{u}(\cdot)\in\Phi$ to (2.2). Let us now choose $M(r,\eta)$ in (2.4) as follows:

$$M(r,\eta) = Q(r,\eta) + K^{*T}(r,\eta)R(r,\eta)K^{*}(r,\eta),\quad r\in S,\ \eta\in Z \tag{A.1}$$

For this choice of $M(r,\eta)$ it immediately follows that the condition (2.4) is satisfied. This proves sufficiency.

To prove the necessary condition, we proceed as follows: Let us assume that steady state solutions $\{\bar{P}_{ik}>0,\ i\in S,\ k\in Z\}$ *do not* exist to (2.12) under the boundary conditions (2.13) for any $Q_{ik}>0$ and $R_{ik}>0$, $\forall i\in S$, $\forall k\in Z$. We need to show that under these conditions, there exist no control law $\bar{u}(x,r,\eta,t)=-K(r,\eta)\bar{x}(t)$, $r\in S$, $\eta\in Z$ to (2.2) that satisfies the condition (2.4).

Let us assume on the contrary that there exists an admissible control law $\bar{u}(\bar{x},r,\eta,t)=-K(r,\eta)\bar{x}(t)$, $r\in S$, $\eta\in Z$ to (2.2) that stochastically stabilizes the control model (2.2). Let us choose $M(r,\eta)>0$ as follows:

$$M(r,\eta) = Q(r,\eta) + K^{T}(r,\eta)R(r,\eta)K(r,\eta),\quad r\in S,\ \eta\in Z \tag{A.2}$$

where $Q(r,\eta)>0$, $R(r,\eta)>0$ $\forall r\in S$ and $\forall\eta\in Z$. Then it follows from the Definition 2.2 that for the above choice of $M(r,\eta)$, there exists a bounded $\tilde{M}>0$ such that condition (2.4) is satisfied. We notice that for $M(r,\eta)$ chosen as in (A.2), the integrand in (2.4) is identical to the function $L(\cdot)$ defined in (2.9). In other words, the control law $\bar{u}(\bar{x},r,\eta,t)=-K(r,\eta)\bar{x}(t)$, $r\in S$, $\eta\in Z$ results in a finite cost for the performance function defined in (2.5). But from Theorem 2.1, we know that the control law (2.11) produces the minimum cost J_{min} for the performance function (2.5). Since steady state solutions $\{\bar{P}_{ik}>0,\ i\in S,\ k\in Z\}$ to the coupled Riccati equations do not exist, this

implies $J_{min}=\infty$. It follows from this that the control law $\bar{u}(\bar{x},r,\eta,t)=-K(r,\eta)\bar{x}(t)$, $r\in S$, $\eta\in Z$ produces a finite cost $J\leq x_0^T\tilde{M}x_0$, $\tilde{M}>0$ is a contradiction. Hence the necessary condition is proven.

ACKNOWLEDGMENT

This work was supported by the Air Force Office of Scientific Research under grant AFOSR-89-0486 DEF.

REFERENCES

CAGLAYAN, A.K., RAHNAMAI, K., MOERDER, D.D., and HALYO, N., 1987, A Hierarchical Reconfiguration Strategy for Aircraft Subjected to Actuator Failure/Surface Damage, Air Force Wright Aeronautics Lab., Wright Patterson AFB, Ohio, AFWAL-TR-87-3034.

HORAK, D.T., 1988, Failure Detection in Dynamic Systems with Modeling Errors, *J. Guidance Control and Dynamics*, **11**, 508-516.

JI, Y., and CHIZECK, H.J., 1990, Controllability, Stabilizability, and Continuous-Time Markovian Jump Linear Quadratic Control, *I.E.E.E. Trans. Autom. Control*, **35**, 777-788.

KRASOVSKII, N.N., and LIDSKII, E.A., 1961, Analytic Design of Controllers in Systems with Random Attributes, Part I-III, *Automn. Remote Control*, **22**, 1021-1025, 1141-1146, 1289-1294.

KUSHNER, H.J., 1967, *Stochastic Stability and Control*, Academic Press, New York.

LOOZE, D., KROLEWSKI, S., WEISS, J., BARRETT, N., and ETERNO, J., 1984, Automatic Control Design Procedures for Restructurable Aircraft Control, NASA Contractor Report CR-172489.

LOOZE, D.P., WEISS, J.L., ETERNO, J.S., and BARRETT, N.M., 1985, An Automatic Redesign Approach for Restructurable Control Systems, *I.E.E.E. Control Systems Mag.*, **5**, 16-22.

MOERDER, D.D., HALYO, N., BROUSSARD, J.R., AND CAGLAYAN, A.K., 1989, Application of Precomputed Control Laws in a Reconfigurable Aircraft Flight Control System, *J. of Guidance, Control and Dynamics*, **12**, 325-333.

SRICHANDER, R., and WALKER, B.K., Stochastic Stability Analysis for Continuous Time Fault Tolerant Control Systems, submitted to *Int. J. Control*.

SWORDER, D.D., 1969, Feedback Control of a Class of Linear Systems with Jump Parameters, *I.E.E.E. Trans. Autom. Control*, **14**, 9-14.

WONHAM, W.M., 1971, Random Differential Equations in Control Theory, in *Probabilistic Methods in Applied Mathematics*, Vol.2, edited by A.T. Bharucha-Reid , Academic Press, New York, 131-212.

Table 1 Summary of design and stability parameters for case (1)

Thresholds	FDI rates	Gains	P_{ik} values	Comments
T_1=1.8	q^1_{12}=0.180	K_1=1.538	P_{11}=0.4235	P_{ik} values converged. Hence the system is stable.
T_2=2.0	q^2_{12}=1.060	K_2=4.225	P_{12}=2.7188	
	q^1_{21}=0.790		P_{21}=0.1588	
	q^2_{21}=0.114		P_{22}=1.3036	

Table 2 Summary of design and stability parameters for case (2)

Thresholds	FDI rates	Gains	P_{ik} values	Comments
T_1=1.2	q^1_{12}=0.575	K_1=1.500	P_{11}=0.4061	P_{ik} values converged. Hence the system is stable.
T_2=0.8	q^2_{12}=2.103	K_2=4.368	P_{12}=2.5783	
	q^1_{21}=2.896		P_{21}=0.2016	
	q^2_{21}=1.059		P_{22}=1.8586	

Table 3 Summary of design and stability parameters for case (3)

Threshold	FDI rates	Gains	P_{ik} values	Comments
T_1=1.2	q^1_{12}=0.575	K_1=1.000	P_{11}=1.03x10^6	P_{ik} values did not converge. System is not stable.
T_2=0.8	q^2_{12}=2.103	K_2=2.250	P_{12}=3.09x10^8	
	q^1_{21}=2.896		P_{21}=6.42x10^5	
	q^2_{21}=1.059		P_{22}=2.63x10^8	

Table 4 Summary of design and stability parameters for case (4)

Thresholds	FDI rates	Gains	P_{ik} values	Comments
T_1=3.0	q^1_{12}=0.067	K_1=1.400	$P_{11}=1.97\times10^{14}$	P_{ik} values did not converge. System is not stable.
T_2=1.5	q^2_{12}=0.114	K_2=2.250	$P_{12}=8.77\times10^{16}$	
	q^1_{21}=1.542		$P_{21}=9.93\times10^{13}$	
	q^2_{21}=0.334		$P_{22}=4.71\times10^{16}$	

Table 5 Summary of design and stability parameters for case (5)

Thresholds	FDI rates	Gains	P_{ik} values	Comments
T_1=1.8	q^1_{12}=0.180	K_1=1.400	P_{11}=0.5377	P_{ik} values converged. Hence the system is stable.
T_2=2.0	q^2_{12}=1.060	K_2=2.250	P_{12}=22.909	
	q^1_{21}=0.790		P_{21}=0.3356	
	q^2_{21}=0.114		P_{22}=16 800	

Captions for Figures

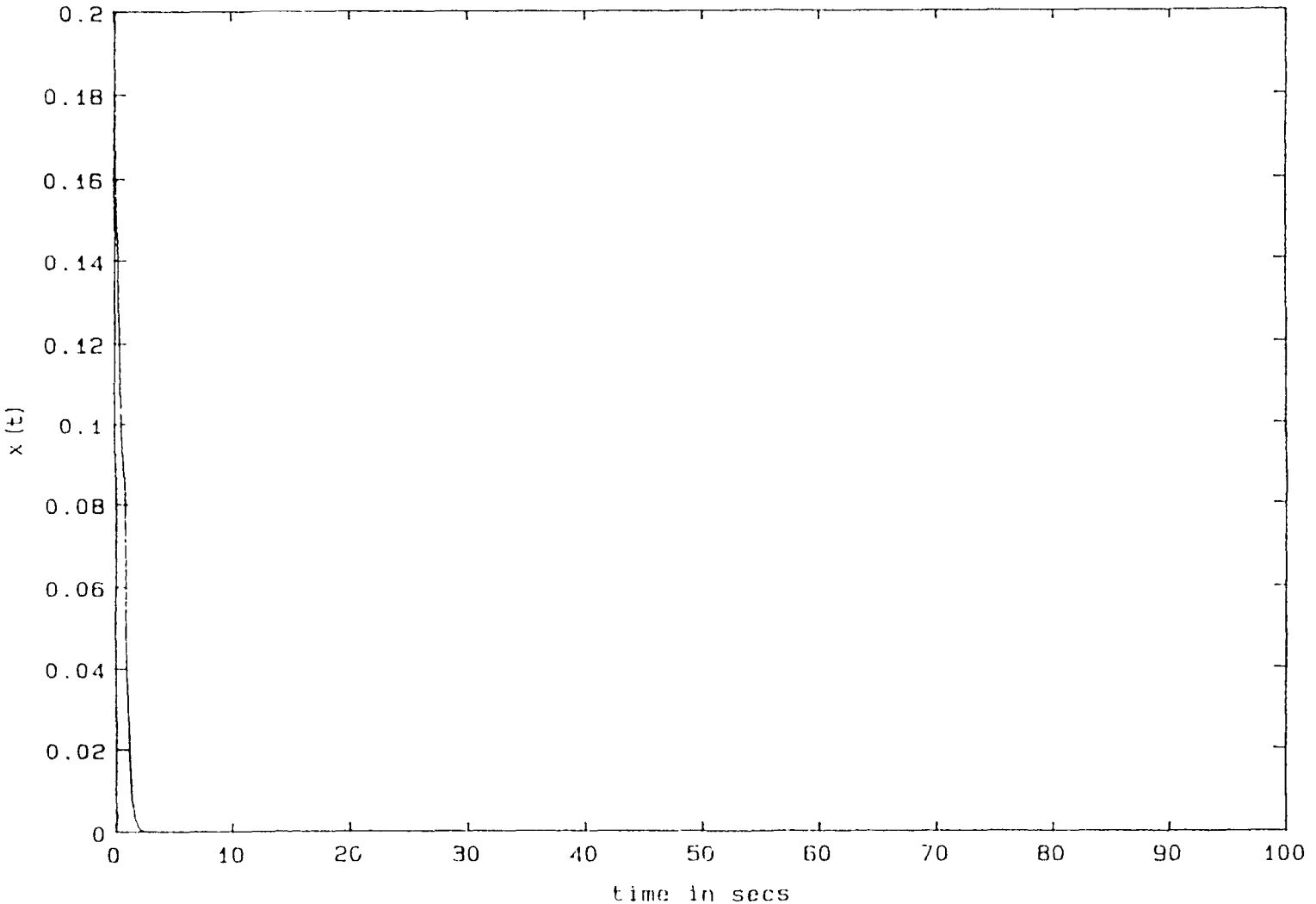
Fig. 1 Example sample function observed during simulation for case (1)

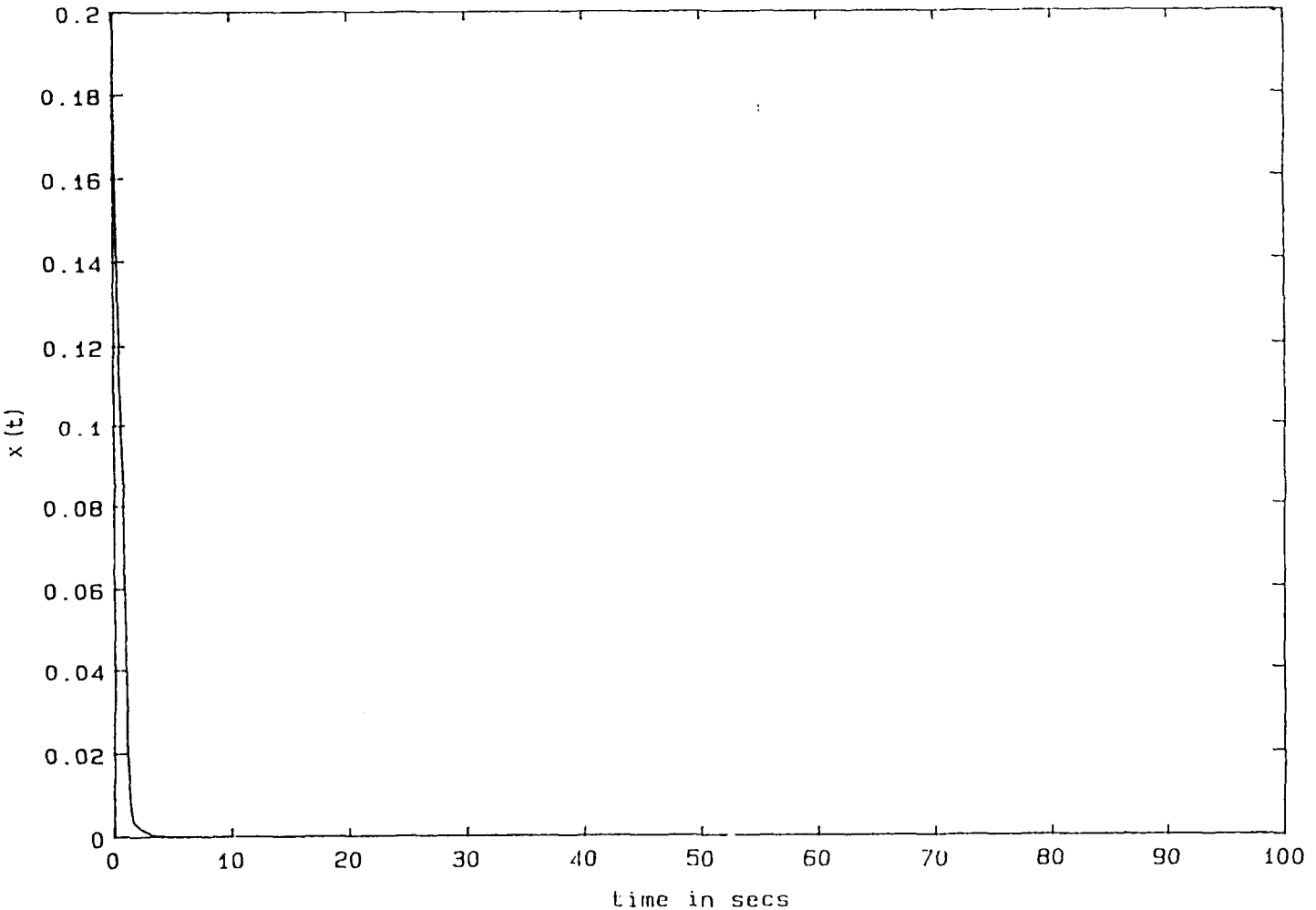
Fig. 2 Example sample function observed during simulation for case (2)

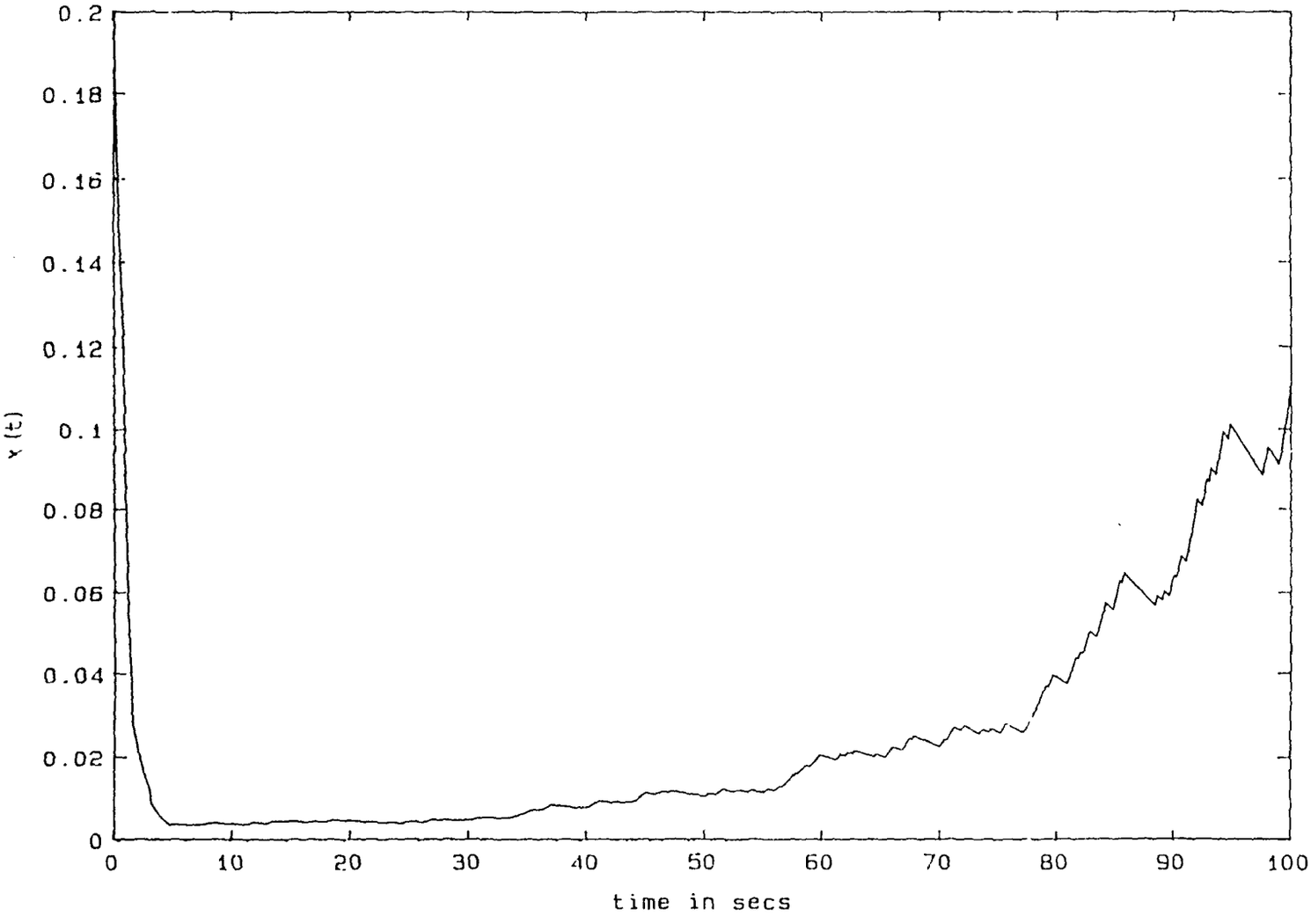
Fig. 3 Example sample function observed during simulation for case (3)

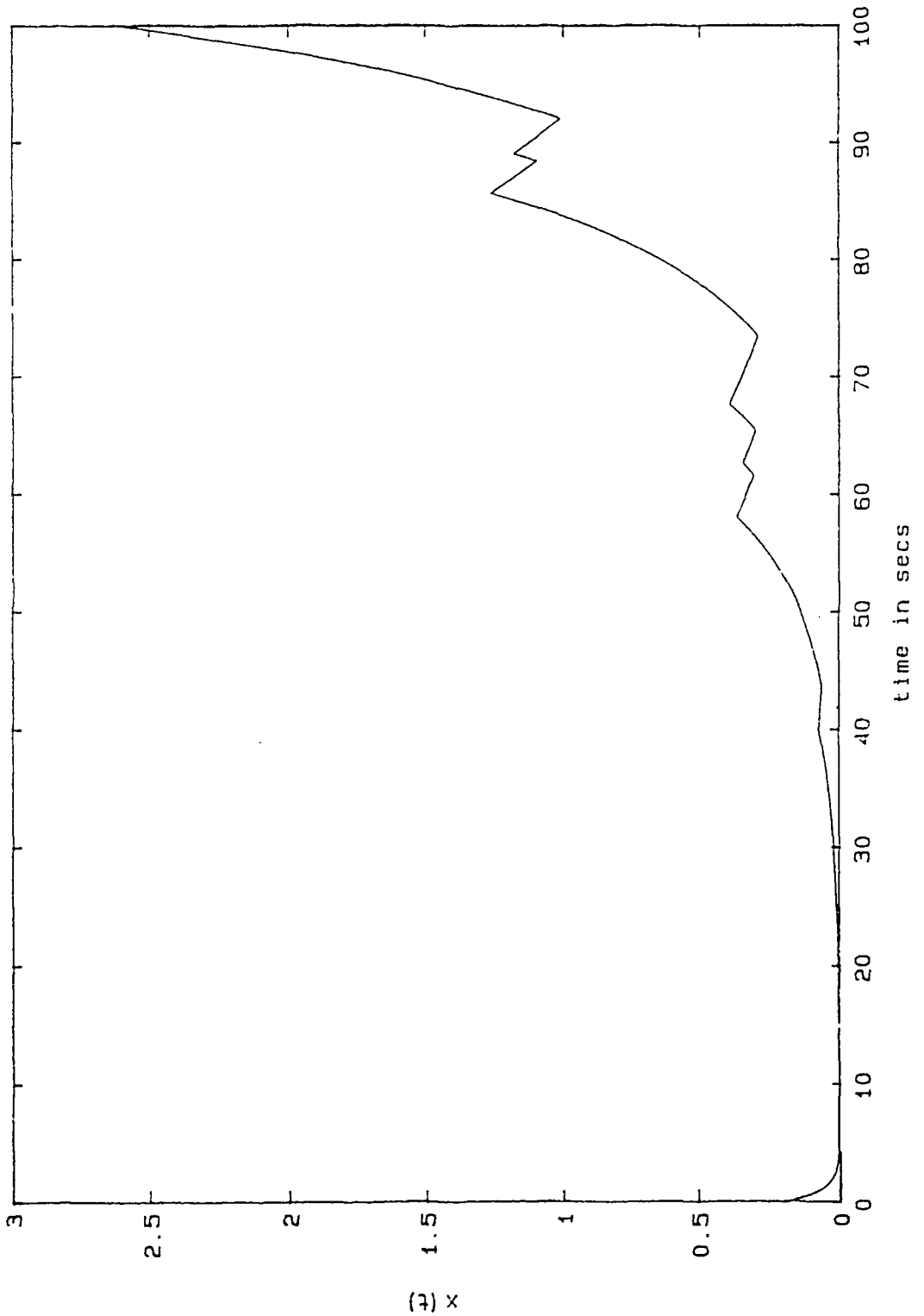
Fig. 4 Example sample function observed during simulation for case (4)

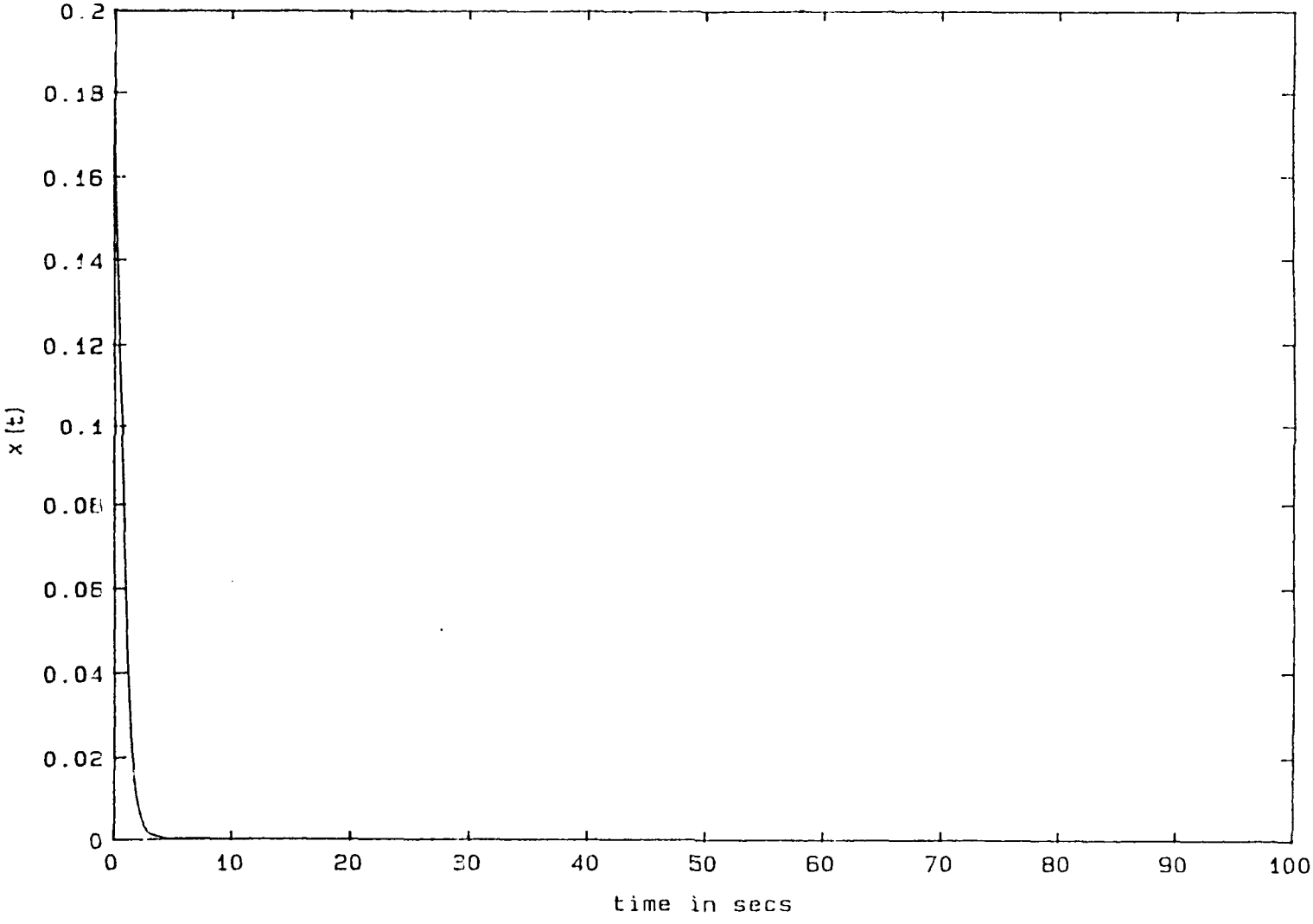
Fig. 5 Example sample function observed during simulation for case (5)


0.2
0.18
0.16
0.14
0.12
0.1
0.08
0.06
0.04
0.02
0
x (t)
0
10
20
30
40
50
60
70
80
90
100
time in secs


0.2
0.18
0.16
0.14
0.12
0.1
0.08
0.06
0.04
0.02
0
x (t)
0
10
20
30
40
50
60
70
80
90
100
time in secs


0.2
0.18
0.16
0.14
0.12
0.1
0.08
0.06
0.04
0.02
0
x (t)
0
10
20
30
40
50
60
70
80
90
100
time in secs


x (t)
3
2.5
2
1.5
1
0.5
0
0
10
20
30
40
50
60
70
80
90
100
time in secs


0.2
0.18
0.16
0.14
0.12
0.1
0.08
0.06
0.04
0.02
0
x (t)
0
10
20
30
40
50
60
70
80
90
100
time in secs

3. SUMMARY OF SIGNIFICANT FINDINGS

The key theoretical findings of this study are primarily the conditions for stochastic stability of FTCS derived in Section 2.2. The results on threshold determination in Section 2.1 and the results on linear state feedback for LTI FTCS in Section 2.3 are of more practical interest.

Summarizing these findings:

For a nonlinear fault tolerant control system subject to random failures with Markovian failure occurrence behavior and with control based upon the decisions of a failure detection system with Markovian decision behavior, the following conditions exist for analyzing its stability:

1. Sufficient conditions exist based upon finding a stochastic Lyapunov function candidate and testing its stochastic time derivative in a particular region of the state space. If this derivative is nonnegative, then almost sure stability in probability of the system is assured. If this derivative is strictly negative, then almost sure asymptotic stability in probability is assured. (See Theorems 4.1 and 4.2 of Section 2.2.)

2. A sufficient condition for exponential stability in mean square of the system is that the Lyapunov function candidate mentioned above be bounded above and below by the scaled L_2 norm of the state vector and that the stochastic time derivative of the Lyapunov function candidate be bounded above by a strictly negative constant times the L_2 norm of the state vector. Furthermore, such a Lyapunov candidate is guaranteed to exist if the system is exponentially stable in mean square. (See Theorems 4.3 and 4.4 of Section 2.2.)

3. If the system is linear and time-invariant, failures affect only the input matrix (or the dynamics matrix) in the state equation, and the control is a linear state feedback with gain dependent only on the decision of the FDI process, then a necessary and

sufficient condition for exponential stability in mean square of the system is that a set of coupled matrix Riccati equations have a finite steady state solution. Furthermore, if the system is exponentially stable in mean square, then it is also almost surely asymptotically stable in probability. (See Theorem 5.1 of Section 2.2.)

The last finding above is particularly significant because it is both necessary and sufficient and is relatively easy to check in practice. Section 2.3 demonstrates this by actually applying this result to a simple fault tolerant system with various state feedback control strategies.

The key finding of the threshold determination study summarized in Section 2.1 is that approximately optimal thresholds for sequential failure detection tests can be found without numerically evaluating the solution to a semi-Markov model of the system behavior. In fact, the approximate optimization is accomplished without even constructing the entire semi-Markov model. The results for one numerical example presented in Section 2.1 show that the performance of thresholds determined by this relatively simple procedure can be very good.

4. PERSONNEL

This research was conducted in its entirety at the University of Cincinnati under the direction of Bruce K. Walker, Associate Professor of Aerospace Engineering and Engineering Mechanics. The research work was performed collaboratively by Dr. Walker and Ramaswamy Srichander, who was a doctoral candidate in Aerospace Engineering and Engineering Mechanics during the period of this grant. Dr. Srichander received his doctorate in September, 1990. Dr. Srichander was supported as a full-time graduate research assistant by this grant from September, 1989, through July, 1990, and then as a full-time postdoctoral research associate during August of 1990.

Except for the manuscripts appearing in Section 2, this report was written entirely by Dr. Walker.

5. PAPERS AND PRESENTATIONS

Several papers and presentations related to the work reported here were completed or submitted during or just after the reporting period. Some of these papers and presentations reported on work that was accomplished primarily under the support of the precedent grants (AFOSR-84-0160 and AFOSR-88-0131). These include:

B.K. Walker, N.M. Wereley, R.H. Luppold, & E. Gai, "Effects of Redundancy Management on Reliability Modeling," IEEE Trans. on Reliability, vol. 38, no. 4, pp. 475-482, October 1989.

N.M. Wereley & B.K. Walker, "Approximate Evaluation of Semi-Markov Chain Reliability Models," Reliability Engineering and System Safety, vol. 28, pp. 133-164, 1990.

N.M. Wereley & B.K. Walker, "Approximate Evaluation of Generalized Markov Health Models of Fault Tolerant Aerospace Systems," pp. 1419-1424 in G. Apostolakis (ed.), Probabilistic Safety Assessment and Management, Elsevier, New York, 1991.

The following papers and presentations were generated as a direct result of this grant:

R. Srichander & B.K. Walker, "Selecting Thresholds for Sequential Fault Detection Tests," to be presented at IFAC SAFEPROCESS'91 Conf., Baden-Baden, Germany, September 1991. (Manuscript appears in Section 2.1.)

R. Srichander & B.K. Walker, "Stochastic Stability Analysis for Continuous Time Fault Tolerant Control Systems," Proc. of 1991 American Control Conf., (Boston), IEEE, New York, pp. 493-501, June 1991. (Manuscript appears in Section 2.2.)

R. Srichander & B.K. Walker, "Stochastic Stability Analysis for Continuous Time Fault Tolerant Control Systems," to appear in Intl. J. of Control, 1992. (Identical to above except for revisions currently in progress.)

B.K. Walker & R. Srichander, "The Synthesis and Stability of a Feedback Control Law for Continuous Time Fault Tolerant Control Systems," to be submitted to Intl. J. of Control, 1991. (Draft manuscript appears in Section 2.3.)

R. Srichander, "Fault Tolerant Control of Continuous Time Ssytems," Ph.D. thesis, Dept. of Aerospace Eng. & Eng. Mechanics, U. Cincinnati, Cincinnati, Ohio, July 1990.

6. REFERENCES

[1] B.K. Walker, N.M. Wereley, R.H. Luppold, & E. Gai, "Effects of Redundancy Management on Reliability Modeling," IEEE Trans. on Reliability, vol. 38, no. 4, pp. 475-482, October 1989.

[2] B.K. Walker, "A Semi-Markov Approach to Quantifying Fault Tolerant System Performance," Sc.D. Thesis, Dept. of Aero. & Astro., Massachusetts Institute of Technology, July 1980.

[3] B.K. Walker, "Performance Evaluation of Systems that Include Fault Diagnostics," Proc. of 1981 Joint Automatic Control Conf.,(Charlottesville, VA), IEEE, New York, June 1981.

[4] B.K. Walker, S.-K. Chu and N.M. Wereley, "Approximate Evaluation of Reliability and Availability Via Perturbation Analysis, Final Technical Report on Grant AFOSR-84-0160," Dept. of Aerospace Eng. & Eng. Mechanics, U. Cincinnati, Cincinnati. Ohio, March 1988.

[5] N.M. Wereley & B.K. Walker, "Approximate Evaluation of Semi-Markov Chain Reliability Models," Reliability Engineering and System Safety, vol. 28, pp. 133-164, 1990.

[6] N.M. Wereley & B.K. Walker, "Approximate Evaluation of Generalized Markov Health Models of Fault Tolerant Aerospace Systems," pp. 1419-1424 in G. Apostolakis (ed.), Probabilistic Safety Assessment and Management, Elsevier, New York, 1991.

[7] R. Srichander & B.K. Walker, "An Approximate Algorithm for Evaluation of Semi-Markov Reliability Models," Proc. of 1989 American Control Conf. (Pittsburgh), IEEE, New York, pp. 2653-2659, June 1989.

[8] B.K. Walker and R. Srichander, "Approximate Evaluation of Reliability and Availability Via Perturbation Techniques, Final Technical Report on Grant AFOSR-88-0131," Dept. of Aerospace Eng. & Eng. Mechanics, U. Cincinnati, Cincinnati, Ohio, July 1989.

[9] B.K. Walker & E. Gai, "Fault Detection Threshold Determination Technique Using Markov Theory," J. Guidance, Control, & Dynamics, vol. 2, no. 4, pp. 313-319, July-August 1979.

[10] B.K. Walker, "Fault Detection Threshold Determination Using Markov Theory," Chap. 7 of P.M. Frank, R.J. Patton, & R.N. Clark (eds.), Fault Diagnosis in Dynamic Systems: Theory and Applications, Prentice-Hall, New York, 1989.

[11] M. Mariton, "Detection Delays, False Alarm Rates, and the Reconfiguration of Control Systems," Intl. J. of Control, vol. 49, pp. 981-992, 1989.

[12] Y. Ji & H.J. Chizeck, "Controllability, Stabilizability, and Continuous Time Markovian Jump Linear Quadratic Control," IEEE Trans. on Automatic Control, vol. AC-35, pp. 777-788, 1990.

[13] (Srichander's thesis, p. 103)